DOCUMENT RESUME

ED 192 092 CE 026 650

TITLE	Nuclear Technology Series. Course 8: Reactor Safety.
INSTITUTION	Center for Occupational Research and Development, Inc., Waco, Tex.: Technical Education Research Center, Waco, Tex.
SPONS AGENCY	Office of Education (DHEW), Washington, D.C.
PUB DATE	May 80
CONTRACT	300-76-0356
NOTE	178p.: For related documents see CE 026 639-672, CE 026 779-780, CE 026 782-785, and CE 026 855-856.
AVAILABLE FROM	Center for Occupational Research and Development, 4800 Lakewood Dr., Suite 5, Waco, TX 76710 (Modules are available individually or by course: write for prices)
EDRS PRICE	MF01 Plus Postage. PC Not Available from EDRS.
DESCRIPTORS	Accident Prevention: Learning Activities: Learning Modules: *Nuclear Energy: Postsecondary Education: Quality Control: *Safety: *Technical Education: Technical Occupations
IDENTIFIERS	Nuclear Energy Occupations: Nuclear Power Plants: *Nuclear Reactors: *Nuclear Technology

ABSTRACT

This technical specialty course is one of thirty-five courses designed for use by two-year postsecondary institutians in five nuclear technician curriculum areas: (1) radiation protection technician, (2) nuclear instrumentation and control technician, (3) nuclear materials processing technician, (4) nuclear quality-assurance/quality-control technician, and (5) nuclear reactor (plant) operator trainee. This course, Reactor Safety, contains five modules: Introduction to Reactor Safety, Reactor Licensing, Reactor Protection Systems, Reactor Emergency Systems, and Safeguards and Security. Each module follows a typical format including the following sections: introduction, module prerequisites, objectives, subject matter, exercises, materials, procedures, data tables, reference materials, and tests. (A master index and suggested program planning guides are also available--see CE 026 856 and CE 026 639-643.) (LRA)

****

* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *

****

ED192092

Nuclear Technology Series

COURSE 8

REACTOR SAFETY

TECHNICAL EDUCATION RESEARCH CENTER-SW
4201 LAKE SHORE DRIVE - SUITE 111
WACO, TEXAS 76710

CE026650

U.S. DEPARTMENT OF HEALTH
EDUCATION & WELFARE
NATIONAL INSTITUTE OF
EDUCATION

THIS DOCUMENT HAS BEEN REPRODUCED EXACTLY AS RECEIVED FROM THE PERSON OR ORGANIZATION ORIGINATING IT. POINTS OF VIEW OR OPINIONS STATED DO NOT NECESSARILY REPRESENT OFFICIAL NATIONAL INSTITUTE OF EDUCATION POSITION OR POLICY

"PERMISSION TO REPRODUCE THIS MATERIAL IN MICROFICHE ONLY HAS BEEN GRANTED BY

D. M. Hull

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

MAY 1980

PREFACE

ABOUT NUCLEAR TECHNOLOGY MODULES

The modules - developed by TERC-SW for use in two-year postsecondary technical institutions to prepare technicians for employment - are useful in industry for updating employees in company-sponsored training, and as laboratory texts in engineering schools. The principles, techniques and skills taught in the modules, based on tasks that nuclear technicians perform, were obtained from a nationwide advisory committee of employers of nuclear technicians. Each module was written by a working technical expert and tested with students.

A module contains the following elements:

Introduction, which identifies the topic and often includes a rationale for studying the material.

Module Prerequisites, which identify the material a student should be familiar with before studying the module.

Objectives, which clearly identify what the student is expected to know for satisfactory module completion. The objectives, stated in terms of action-oriented behaviors, include such action words as operate, measure, calculate, identify and define, rather than words with many interpretations, such as know, understand, learn and appreciate.

Subject Matter, which presents the background theory and techniques supportive to the objectives of the module. Subject matter is written with the technical student in mind.

Exercises, which provide practical problems to which the student can apply this new knowledge.

Materials, which identify the equipment required to complete the laboratory procedure.

Procedures, which is the experiment section, or "hands-on" portion of the module (including step-by-step instruction) designed to reinforce student learning.

Data Tables, which are included in most modules for the first year (or basic) courses to help the student learn how to collect and organize data.

Reference Materials, which are included as suggestions for supplementary reading/viewing for the student.

Test, which measures the student's achievement of the prestated objectives.

Copyright in 1977 by the Technical Education Research Center, Inc. Printed in the United States of America. All rights reserved. These materials, or parts thereof, may not be reproduced in any form without permission.

The materials contained herein were developed pursuant to a contract with the Office of Education, U.S. Department of Health, Education and Welfare: Contract No. 300760356. Contractors undertaking such projects under Government sponsorship are encouraged to express freely their professional judgment in the conduct of the project. Points of view or opinions stated do not, therefore, necessarily represent official Office of Education position or policy.

The Nuclear Technology Series will consist of five curricula when completed:

- Nuclear Reactor (Plant) Operator Trainee.
- Radiation Protection Technician.
- Nuclear Materials Processing Technician.
- Nuclear Quality-Assurance/Quality-Control Technician.
- Nuclear Instrumentation and Control Technician.

The completed Nuclear Reactor (Plant) Operator Trainee curriculum consists of the following sixteen technical specialty courses made up of 114 instructional modules:

- Radiation Physics.
- Radiation Protection I.
- Principles of Process Instrumentation.
- Heat Transfer and Fluid Flow.
- Introduction to Nuclear Systems.
- Instrumentation and Control of Reactors and Plant Systems.
- Reactor Operations.
- Reactor Safety.
- Reactor Auxiliary Systems.
- Power Plant Systems.
- Radiation Detection and Measurement.
- Reactor Physics.
- Power Plant Chemistry.
- Introduction to Quality Assurance/Quality Control.
- Metallurgy and Metals Properties.
- Mechanical Component Characteristics and Specifications.

Availability: Instructional modules are available individually or by courses from:

Technical Education Research Center - Southwest
4201 Lake Shore Dr., Suite 111
Waco, Texas 76710
Telephone (817) 772-8756

Printed:

CONTENTS

Preface

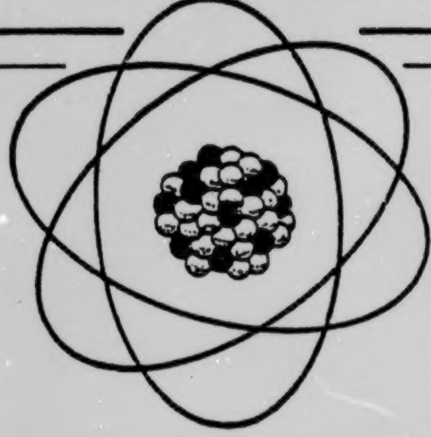
Module 8-1 Introduction to Reactor Safety

Module 8-2 Reactor Licensing

Module 8-3 Reactor Protection Systems

Module 8-4 Reactor Emergency Systems

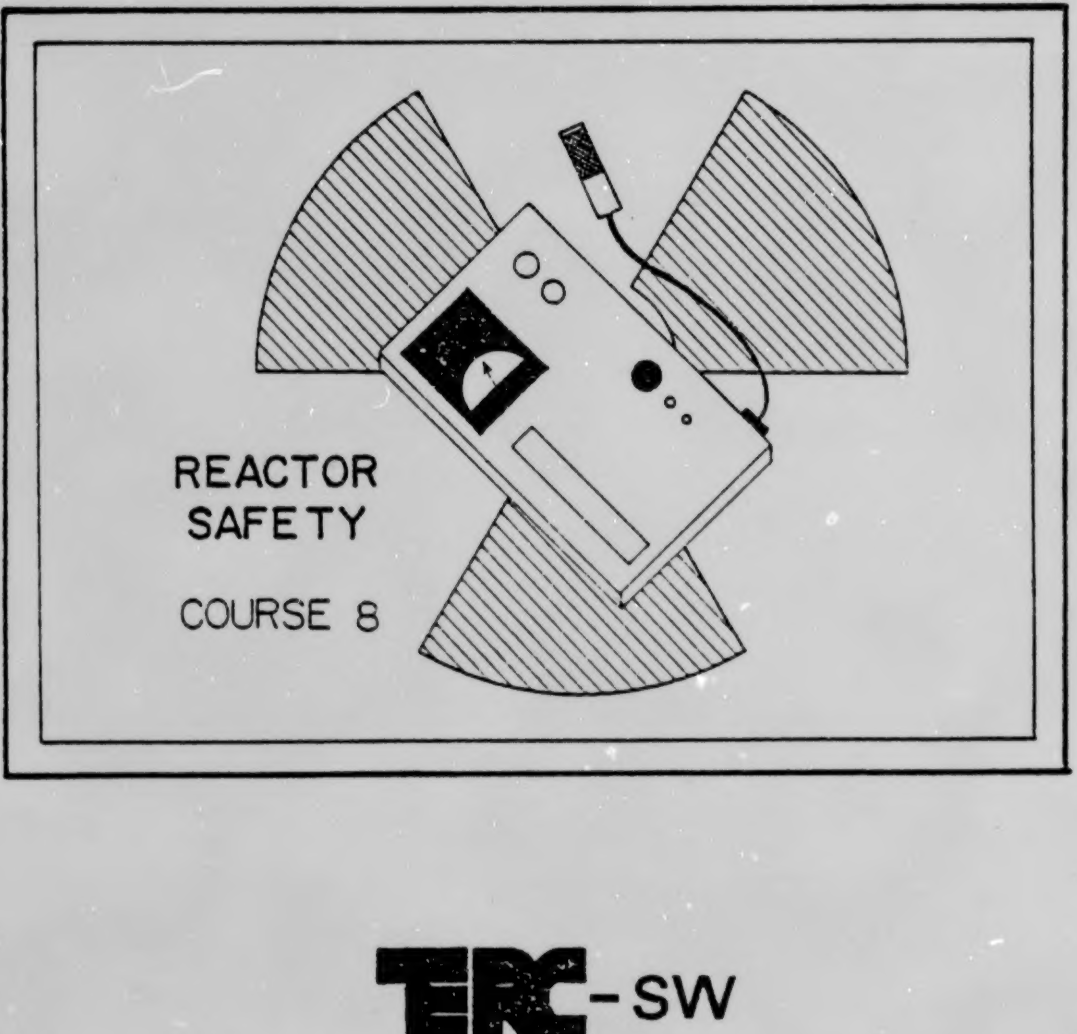
Module 8-5 Safeguards and Security



NUCLEAR TECHNOLOGY

MODULE 8-1 INTRODUCTION TO REACTOR SAFETY. -

RONALD L. KATHREN
PORTLAND GENERAL ELECTRIC COMPANY


REACTOR
SAFETY
COURSE 8

TERC-SW

TECHNICAL EDUCATION RESEARCH CENTER — SOUTHWEST
4201 LAKE SHORE DRIVE WACO, TEXAS

COURSE MODULES

COURSE 8 REACTOR SAFETY

MODULE 8-1	Introduction to Reactor Safety
MODULE 8-2	Reactor Licensing
MODULE 8-3	Reactor Protection Systems
MODULE 8-4	Reactor Emergency Systems
MODULE 8-5	Safeguards and Security

Copyright in 1977 by the Technical Education Research Center, Inc. Printed in the United States of America. All rights reserved. These materials, or parts thereof, may not be reproduced in any form without permission.

The materials contained herein were developed pursuant to a contract with the Office of Education, U.S. Department of Health, Education and Welfare: Contract No. 300760356. Contractors undertaking such projects under Government sponsorship are encouraged to express freely their professional judgment in the conduct of the project. Points of view or opinions stated do not, therefore, necessarily represent official Office of Education position or policy.

Technical Education Research Center
Southwest
4201 Lake Shore Drive, Suite 111
Waco, Texas 76710

INTRODUCTION

Nuclear reactors incorporate special backup safety systems to prevent (or minimize the consequences of) accidents. This defense-in-depth concept dates back to December 2, 1942, when the first manmade reactor (CP-1) was being prepared for startup in a squash court under Stagg Stadium at the University of Chicago. It was equipped with three sets of control rods for varying the level of operation.

The first set of automatic safety rods was controlled by small electric motors. A second set, to be used as emergency safety rods (nicknamed "Zip") were heavily weighted at one end and held in place above the core by a rope tied to the viewing balcony. If the automatic safety rods failed, a scientist standing by with an axe was to cut the rope so the emergency rods could drop, by gravity, and shut down the reactor.

Actual power control of the reactor was achieved by a third control-rod set, manually operated by another scientist under orders from the director, Enrico Fermi.

In addition to the triple system of control rods, CP-1 had a fourth, totally independent shutdown system. A three-man liquid control squad, poised on a platform above the reactor, stood ready to flood the core with a cadmium solution in the event all the control-rod systems failed.

In the 35 years since the startup of CP-1, reactors have grown in size and complexity. With this growth, an entirely new field of reactor safety has developed.

This module provides a basic introduction to reactor safety philosophy, an examination of potential hazards and consequences of reactor accidents, legal and regulatory basis of reactor safety, as well as review of accident experience and predictive evaluations.

MODULE PREREQUISITES

The student should have a basic understanding of reactor operations and design, radiation protection and basic radiation physics, as might be obtained by completion of Courses 1, "Radiation Physics," 2, "Radiation Protection," 5, "Introduction to Nuclear Systems," and 7, "Reactor Operations." Knowledge of instrumentation, control systems and basic statistics is necessary.

OBJECTIVES

Upon completion of this module, the student should be able to:

1. List three main criteria of basic reactor safety philosophy; relate each criterion to the design, construction and operation of a nuclear power plant.
2. Define the following terms relative to reactor safety:
    Defense-in-depth.
    Negative temperature coefficient of reactivity.
    Containment vessel or structure.
    Redundancy.
    Emergency core cooling system (ECCS).
    Contingencies (unforeseen events).
    Design basis accident (DBA).
    Quality assurance/quality control.
    Site factors.
    Exclusion area.

9

Low-population zone.
Accident classification.
Loss-of-coolant accident (LOCA).
Reactor safety study (Rasmussen Report).
Fault-tree analysis.

3. List four major, multiple barriers designed into power reactors to reduce consequences of accidents.
4. Explain the three levels of safety program implementation.
5. State meaning and consequence(s) of each accident category; explain basic differences between accident classes.
6. List four potential hazards associated with postulated accidents; give their source and tell how they could affect environment.
7. Sketch a simple event fault tree.
8. Calculate total probability of an event (from a list of probabilities for individual component failure occurrences).

PHILOSOPHY OF REACTOR SAFETY

General safety philosophy rests on several assumptions and principles. It is impossible to design and plan for all things that might occur; therefore, practical considerations that enter into basic safety philosophy are generally developed by considering benefits to be gained versus risks. Designs should be kept as inherently safe and simple as practical, recognizing that no one system or body of knowledge can ensure with certainty the reduction of risks to zero. Structures and materials must not operate at their limits of capability, but must have adequate safety margins based on conservatism, and rest on sound established principles. When in doubt, the more conservative path must be chosen; this is the cornerstone of safety.

Nuclear reactors - whether large power reactors or small research reactors - adhere to the same basic safety philosophy and design. They are built and operated in accordance with established engineering codes and standards employing specific legal and regulatory criteria. Basic safety philosophy incorporates these three criteria:

Inherently safe designs.
Multiple barriers.
Multiple and redundant safety systems.

INHERENTLY SAFE DESIGNS

Inherent safety in design dictates use of fail-safe physical features. These features ensure safe shutdown so that large unanticipated upsets can be tolerated without major damage to the reactor systems, and without producing hazards to the public or environment.

Inherently safe design features include such items as suspension of control and safety rods by electromagnets. If there is a power failure, magnetic contact is lost and the rods fall by gravity back into the core, shutting down the reactor in a fail-safe manner; i.e., in the event of some failure (in this case, failure of the electrical power supply), a safe situation occurs.

The particular fail-safe design used in this example has many elements. First, it takes advantage of gravity, a physical phenomenon that is a certainty in a static system. The reactor, of course, must be appropriately designed so that downward insertion of rods shuts off the reactor, allowing the law of gravity to prevail. Obviously, lateral (sideways) insertion or pushing the rods upward to turn off the reactor is not as sure or simple as downward free fall.

An equally important, inherently safe design feature employs the negative temperature coefficient of reactivity ($-\Delta T/k$) designed into all American power reactors. In such reactors the core has less reactivity as it heats up, so it tends to shut itself off as the power level increases. Most research reactors and all power reactors are designed so that the negative temperature coefficient is great enough to effectively provide an upper limit on power level as well as help prevent power excursions.

The negative temperature coefficient of reactivity can be an effective control of a situation in which a sudden large increase in reactivity has occurred, as might be the case if a control rod were removed too quickly.

MULTIPLE BARRIERS

The use of multiple barriers to prevent escape of radioactive substances to the environment is common to all reactors. Power reactors usually have at least four such barriers:

Fuel.
Cladding.
Reactor vessel.
Containment vessel.

The first innermost barrier is the fuel itself. It tends to hold or trap fission products and incorporated transuranium elements (those having an atomic number > 92). Only gaseous fission products show any appreciable diffusion through the fuel barrier.

The second barrier is the cladding around the fuel elements themselves. Although the cladding is relatively thin, it contains the fission products.

Although coolant liquid (moderator) might be considered a barrier (or at least a partial barrier) to the escape of radioactive substances, in certain severe postulated accidents, or in the case of gas-cooled reactors, there may be no liquid in which the radioactive substances could be dissolved or mechanically entrapped; therefore, the third barrier is generally considered to be the reactor vessel itself.

The final, or fouth, barrier is the containment vessel, which serves to keep the radioactive substances inside should the other systems fail.

MULTIPLE AND REDUNDANT SAFETY SYSTEMS

The concept of multiple barriers is an example of the defense-in-depth philosophy, which extends to all reactor systems and operations. This philosophy is better explained by the third criteria, multiple and redundant safety systems. Multiplicity of safety systems is characterized by a whole series of systems operating on different principles for different reactor conditions. Thus, barriers to prevent escape of radioactive products, and a standby electrical system and safety injection system (i.e., boron solution to control reactivity) represent a multiplicity of safety systems.

The redundancy concept goes hand-in-glove with, but does not replace, the multiple safety system concept. Redundant, as defined in the dictionary, means "excessive or exceeding what is usual." This definition also applies to redundancy in reactor safety. The CP-1 reactor had three systems of redundant safety rods that could shut down the reactor. (It also had a multiplicity of shutdown systems: the control-rods systems and the cadmium poison solution.)

Redundancy can extend down to any system level. For example, two or more monitoring systems for the same effluent tank, two or more motor-operated valves to control flow, double or triple demineralizers and tandem-mounted diesels to drive one of two emergency power generators.

Redundant systems serve as backup or standby systems usually performing the same function for the same response and in the same manner as the primary system they may be called upon to replace.

The difference between multiplicity and redundancy may become obscured or fuzzy, particularly when a large power reactor is being examined. Simplified diagrams illustrate the concepts of redundancy (Figure 8-1-1) and multiplicity (Figure 8-1-2).

Redundancy, in an emergency core cooling system (ECCS),

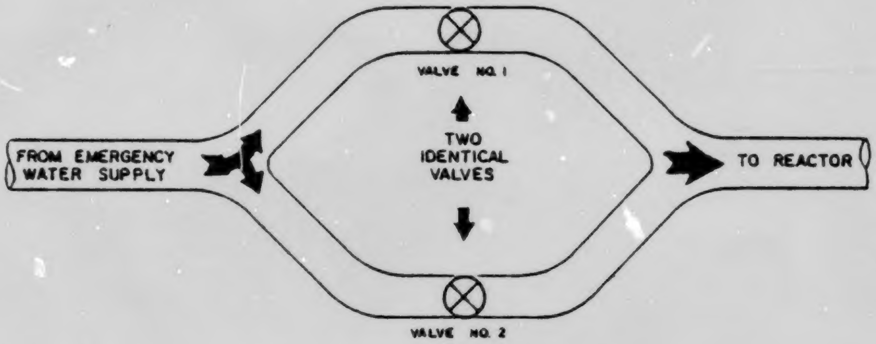

VALVE NO. 1
FROM EMERGENCY WATER SUPPLY
TWO IDENTICAL VALVES
TO REACTOR
VALVE NO. 2

Figure 8-1-1. Two identical valves exemplify a redundant system.

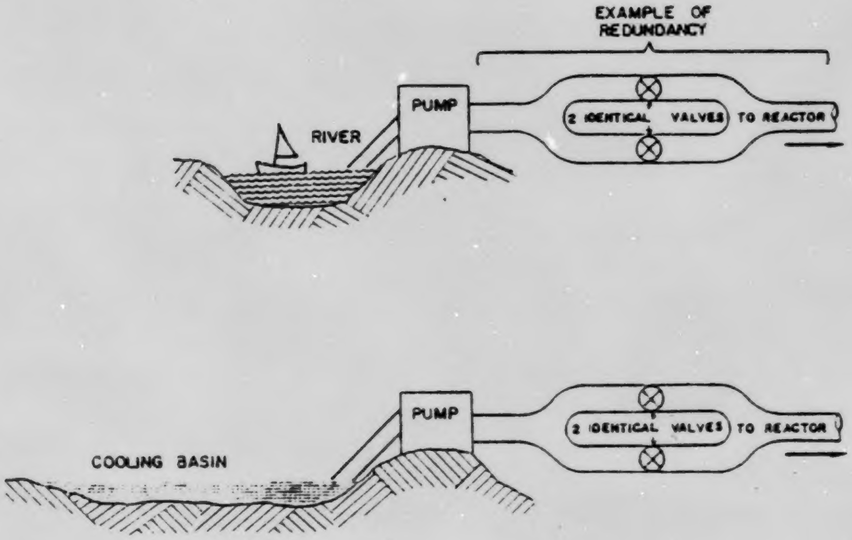

EXAMPLE OF REDUNDANCY
PUMP
RIVER
2 IDENTICAL VALVES
TO REACTOR
PUMP
COOLING BASIN
2 IDENTICAL VALVES
TO REACTOR

Figure 8-1-2. Two different water supplies form a multiple system. (Note redundant supply line.)

provides two equivalent valves and paths, but only one valve has to open for the system to work.

In the emergency core cooling system, multiples are again used as an example. Two different sources of emergency water are provided, one from a river and the other from a cooling basin. Either is a complete, separate source of water; hence, the two are multiple rather than redundant.

Note, also, how redundant and multiple components may be combined (Figure 8-1-3) into a system designed to provide

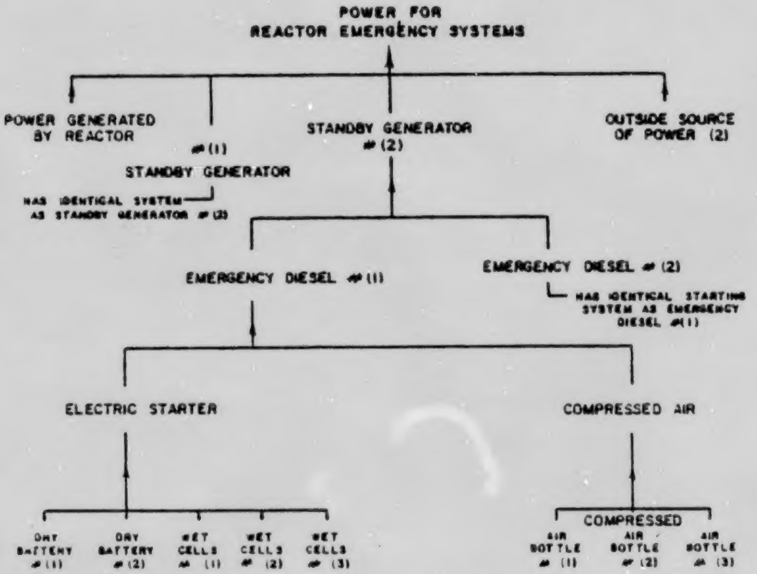

POWER FOR
REACTOR EMERGENCY SYSTEMS
POWER GENERATED BY REACTOR
#(1) STANDBY GENERATOR
HAS IDENTICAL SYSTEM AS STANDBY GENERATOR #(2)
STANDBY GENERATOR #(2)
OUTSIDE SOURCE OF POWER (2)
EMERGENCY DIESEL #(1)
EMERGENCY DIESEL #(2)
HAS IDENTICAL STARTING SYSTEM AS EMERGENCY DIESEL #(1)
ELECTRIC STARTER
COMPRESSED AIR
DRY BATTERY #(1)
DRY BATTERY #(2)
WET CELLS #(1)
WET CELLS #(2)
WET CELLS #(3)
COMPRESSED
AIR BOTTLE #(1)
AIR BOTTLE #(2)
AIR BOTTLE #(3)

Figure 8-1-3. Multiple and redundant systems.

power for reactor emergency systems. At the first level, power for reactor emergency systems can be supplied by three separate sources. At least two of these sources are identical or redundant. Each redundant standby generator is powered by two diesels, either one of which is sufficient; hence, there is again redundancy. The diesels can be started by either compressed air or electric starters - multiple starters for each. The electric starters can be energized by either of two dry batteries (redundancy) or several wet cells, providing both multiplicity and redundancy at this level.

IMPLEMENTATION OF A SAFETY PROGRAM

The basic safety philosophy discussed above is implemented throughout the design, construction and operation of a nuclear reactor. In the design phase, the defense-in-depth concept is implemented by application of three levels of safety.

First-level objective: "To provide the best possible design of quality, requisite construction, and appropriate operational facility."

The first level, based on maximum safety during normal operation, includes maximum tolerance to system malfunction. It includes ensuring that inherent or builtin reactor characteristics are stability and safety. It also assumes specification of the best available materials and compounds, as verified by tests and measurements.

Safety margins must include provision for possibly degrading stresses peculiar to reactors, such as radiation effects on materials. Provision must also be made for monitoring of operations and systems that involve reactor safety or safety of the facility as a whole.

Generally, the first level of design safety dictates incorporation of high quality standards, and engineering practices with freedom from error and maximum attention to detail, all of which eliminate or minimize failures and operational errors.

Second-level objective: "To assume that, in spite of the best possible effort on the first level, accidents will occur; thus, safety systems must be included to prevent or minimize the negative aspects of such accidents."

Despite best efforts at the first level, situations may occur that might endanger the public, the environment or the reactor; hence, additional safety systems must be included to protect public and operators, as well as to prevent or minimize damage from such events.

For example, two separate and independent systems may be used to achieve one purpose. More specifically, engineered limits on the degree of motion or speed of fuel control rods may be indicated. Two or more independent electric power cables, physically separated by a fireproof barrier, may be used as an engineered safeguard to provide that, in the event of a fire affecting one, the other(s) would still be functional.

Third-level objective: "To assume that, in spite of the second level, accidents or contingencies (unforeseen events) may still occur and, therefore, containments must be provided for loss of radioactive substances."

The third level of design safety incorporates appropriate additional safety systems. These systems are based on evaluation of postulated accidents in which engineered safety or protective systems fail at the same time an accident occurs (the accident they are designed to control). Major or catastrophic natural events (floods, earthquakes, storms) are considered, as are simultaneous failure of two or more independent/redundant safety systems. Thus, stress limits on containment structures may be adjusted, or emergency core cooling systems made oversize, to protect against these design basis accidents (DBA's).

Implementation of basic safety philosophy during the design phase requires an extraordinary degree of thoroughness. What is being done must be checked continually against plans and specifications. It also requires rigid adherence to codes and standards, as well as criteria for materials, construction personnel and the work performance; therefore, in the construction of a nuclear power plant, a full-scale quality-assurance program is mandatory.

Quality assurance (QA) is the set of activities necessary to ensure that the end product performs satisfactorily in service. Quality assurance includes quality control (QC). Quality control is the testing and verification of performance and materials. It includes inspection for performance, and specification and nondestructive testing of components, assemblies and completed work.

Quality control utilizes such methods as radiography, dye-penetrant measurements and magnaflux techniques. Quality assurance basically ensures the adequacy of the design, and that both construction methodology and specified components are in conformance with the design. Also, the quality-assurance program functions to ensure that adequate records are kept, and that all design changes, test results and similar information are current, appropriately documented and retrievable.

Quality-assurance program criteria are required by Nuclear Regulatory Commission (NRC) regulations. These requirements list eighteen basic criteria in Appendix B of Title 10 Code of Federal Regulations (CFR), Part 50, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants." Design criteria are spelled out in 10CFR50, Appendix A, "General Design Criteria for Nuclear Power Plants," which includes, among its sixty-four criteria, specific design features to ensure that basic safety philosophy is followed.

Implementation of safety philosophy in the operational phase is accomplished by a rigid pre-operational testing program for personnel and physical facilities. Personnel must meet specific standards with respect to training and qualification. Operation of the reactor is restricted to personnel who have demonstrated their capability by passing a rigid examination administered by the NRC.

The operator's examination includes written, oral and operational portions. If a candidate successfully passes the examinations, NRC issues a license valid for a two-year period. The license is normally specific to a single reactor. Another test must be satisfactorily passed prior to license renewal. Normally, two licensed operators - one possessing a senior operator's license - must be present in the control room during operation. Specific requirements for the number and class of operators are included in the Technical Specifications, which are a part of the Reactor License approval documents.

In addition to these personnel qualifications, the reactor undergoes a thorough testing program prior to operation to verify performance of components and systems.

All safety systems and components are rigorously tested in accordance with pre-established written procedures. These procedures include, but are not limited to, signed check-off lists, and verifications and recordings of all data for comparison with design specifications.

The rigid pre-operational testing program fulfills many purposes, including verification that safety-related components, equipment and systems meet design objectives.

REACTOR SITING

An important consideration in physical safety is reactor location with reference to population centers, other man-made facilities and natural features that might be harmed in the event of a serious accident. Of greater significance, perhaps, is the potential impact of the site itself on the safety of the reactor, especially with respect to the consequences of accidents.

The many specific site factors that must be considered in a safety evaluation process are contained in 10CFR100, "Reactor Site Criteria." These factors include the area of the site, site location with respect to population centers, population density and land use, and the ecology, geology, seismology, meteorology and hydrology of the site and surrounding area.

The last four "ologies" are particularly significant from the standpoint of physical safety:

Geology.
Seismology.
Meteorology.
Hydrology.

Site geology is important in design of the foundation and structure (i.e., ground strata must be stable and free from conditions that could lead to shifting or settling).

For obvious safety reasons, a reactor should not be located over or close to an active geological fault; thus, seismology is an extremely significant consideration.

In the event of an accidental release of radioactive products, meteorological (weather) conditions can affect, to a great extent, where the radioactive products travel and how much is deposited in a given area. The probability of tornados or typhoons may dictate special construction to ensure that the reactor can withstand such unusual forces with no compromise of safety.

Finally, an evaluation of the hydrology of the region provides insight into potential flood situations. It allows a site to be selected to minimize hazards from this source. Hydrology can also provide information regarding waterborne distribution of radioactive products.

An exclusion area (Figure 8-1-4) is that area in which an individual could receive a whole body dose equivalent of 25 rem (rem is the unit of biological dose) or a thyroid dose from radioiodines of 300 rem within the first two hours following the most severe postulated accident. The reactor owner maintains control over the exclusion area. This area must be capable of complete evacuation within a two-hour period. Only in rare instances is residence allowed in the exclusion area. And, as a practical matter, dwellings or overnight stays (including campgrounds) are not permitted.

The low-population zone is the area in which an individual would receive a total lifetime whole body dose of 25 rem, or a thyroid dose of 300 rem from radioiodines. The purpose of establishing both the exclusion area and the low-population zone is protection of the public in the

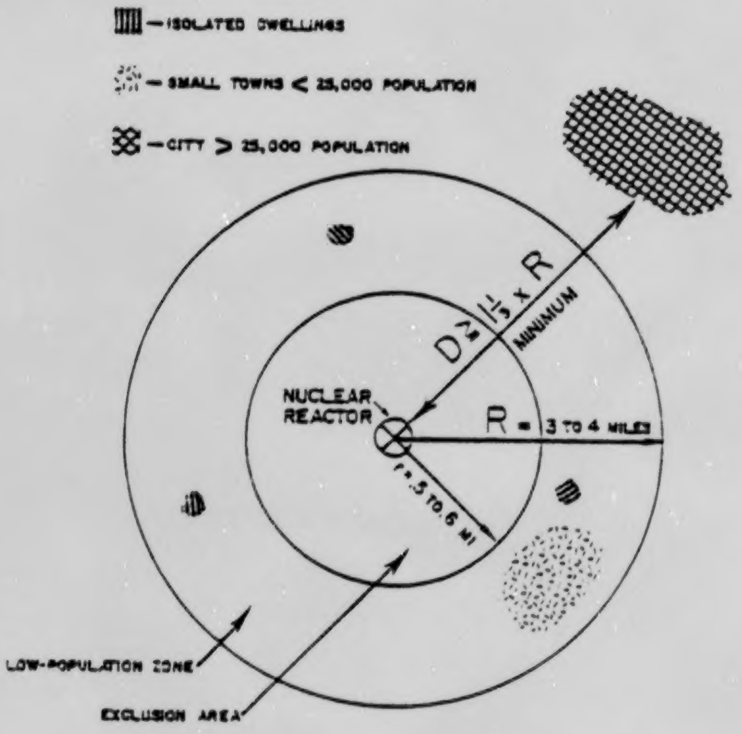

—ISOLATED DWELLINGS
— SMALL TOWNS < 25,000 POPULATION
—CITY > 25,000 POPULATION
D ≥ 1⅓ x R
MINIMUM
NUCLEAR REACTOR
R = 3 TO 4 MILES
r = .5 TO .6 MI
LOW-POPULATION ZONE
EXCLUSION AREA

Figure 8-1-4. Approximate relationship between location of nuclear reactor and surrounding population.

event of a DBA.

An additional siting consideration is the population center distance, which is the distance from the reactor to the nearest densely populated area (city) with more than about 25,000 inhabitants. This distance must be at least 1-1/3 times the low-population zone distance. Again, the purpose is to minimize the total population in the event of a DBA.

In most safety analyses of large power reactors, the exclusion area turns out to have a radius of about 800 to 1000 meters (0.5 to 0.6 mile), and this figure is frequently used for planning purposes. The size of the low-population zone is more variable. It generally runs three to four miles, although it can be larger in some instances.

EVALUATION OF POSTULATED ACCIDENTS

("Postulated," in this sense, means hypothetical or made up.)

Assessment of nuclear reactor safety is accomplished by evaluating the consequences of a series of hypothetical DBA's determining, in part, any risk to the public. These evaluations include analyses of design, performance and failures of structures, systems and components. Particular emphases is placed on adequacy, with respect to prevention, control and minimization of hazards from accidents and their consequences.

The analyses are performed over a wide range of events. (Relatively small and insignificant occurrences might take place occasionally with no release of radioactivity to the environment. Potentially serious accidents of extremely low likelihood could release radioactivity from the reactor facility to the environment.) Minor, moderate-frequency events might include any partial loss of normal reactor coolant flow, loss of off-site electrical power, failure of a single safety rod to perform emergency shutdown (scram) and excessive load increase.

Accidents with small probability of occurrence (in which an abnormal release of radioactive substances to the environment is possible, but not likely), include minor breaks and leaks in pipes and valves in primary or secondary coolant systems, demineralizer leaks or losses of coolant flow.

The most severe postulated accidents are also highly unlikely. They include DBA's based on extremely rare, severe floods or storms, earthquakes, losses of coolant, control-rod ejections and sabotage.

Since detailed evaluation of all possible accidents is both impossible and unnecessary, the broad range of accidents has been divided into nine accident classifications (Table 8-1-1).

(Class 9 accidents are considered so improbable as to be essentially impossible, and are not normally considered for analysis.)

THE REACTOR SAFETY STUDY

The single most comprehensive safety study ever performed is called the Rasmussen Report. This 15-volume analysis of light-water reactor safety was prepared under the direction of Professor Norman C. Rasmussen of MIT. It required 50 person years to complete, and cost three million dollars. The report was initially released in draft form on August 20, 1974, seventeen years after its pioneering precedessor, WASH-740.

The WASH-740 report, issued in 1957, was prepared for the Atomic Energy Commission (AEC) by a team of experts

TABLE 8-1-1
CLASSIFICATION OF POSTULATED ACCIDENTS AND OCCURRENCES

CLASS	DESCRIPTION	EXAMPLE(S)
1	Insignificant Incidents	Small spills Small leaks inside containment
2	Misc. small releases outside Containment	Spills Leaks and pipe breaks
3	Radwaste System Failures	Equipment failure Serious malfunction or human error
4	Release of Radioactivity into the Primary System	Fuel defects during normal operation Transients outside expected range of variables
5	Release of Radioactivity into Secondary System	Class 4 and Heat Exchanger Leak
6	Refueling Accidents Inside Containment	Drop fuel element Drop heavy object onto fuel Mechanical malfunction or loss of cooling in transfer tube
7	Accidents to Spent Fuel Outside Containment	Drop fuel element Drop heavy object onto fuel Drop shielding cask - loss of cooling to cask, transportation incident on site
8	Accident Initiation Events considered in Design-Basis	Reactivity Transient Rupture of Primary Piping (LOCA) Flow Decrease - Steamline Break
9	Hypothetical Sequences of Failures More Severe than Class 8	Successive Failures of Multiple Barriers normally provided and maintained

(Adapted from WASH-1250)

and consultants from Brookhaven National Laboratory. This study, completed prior to operation of commercial power reactors in the United States, undertook to predict the extent of damage from a catastrophic accident in an "uncontained," large nuclear power plant. Extreme assumptions were used to estimate fatalities, injuries and property damage; from these estimates, insurance liability limits were deduced.

The WASH-740 study, however, had several serious defects, including, in its basis, a lack of commercial operating experiences, a series of overly pessimistic circumstances and several possibly unrealistic assumptions. Hence, the Rasmussen study, begun in 1972, has supplemented the earlier WASH-740 analysis through the inclusion, in the main, of operating experiences.

The final version of the Rasmussen Report, officially called Reactor Safety Study and designated WASH-1400, was issued in October, 1975, after critique of the draft by numerous outside parties. These parties included Environmental Protection Agency (EPA), American Physical Society (APS), Union of Concerned Scientists and other appropriate groups. The study used "event-tree" (an event tree defines paramaters or limits of an initial failure) and fault-tree analysis techniques to establish hypothetical accident conditions, and to estimate probabilities.

A fault-tree analysis establishes the ways in which a defined failure can occur. Fault-tree analyses consider the range of accident possibilities for an event by evaluating the many component and failure modes that might occur.

To illustrate a simple fault-tree/event-tree analysis, consider a situation in which it is necessary to ascertain if a two-cell flashlight will, in fact, work properly (Figure 8-1-5). Inspection of the flashlight shows four major components:

A switch.
Two batteries.
A bulb.

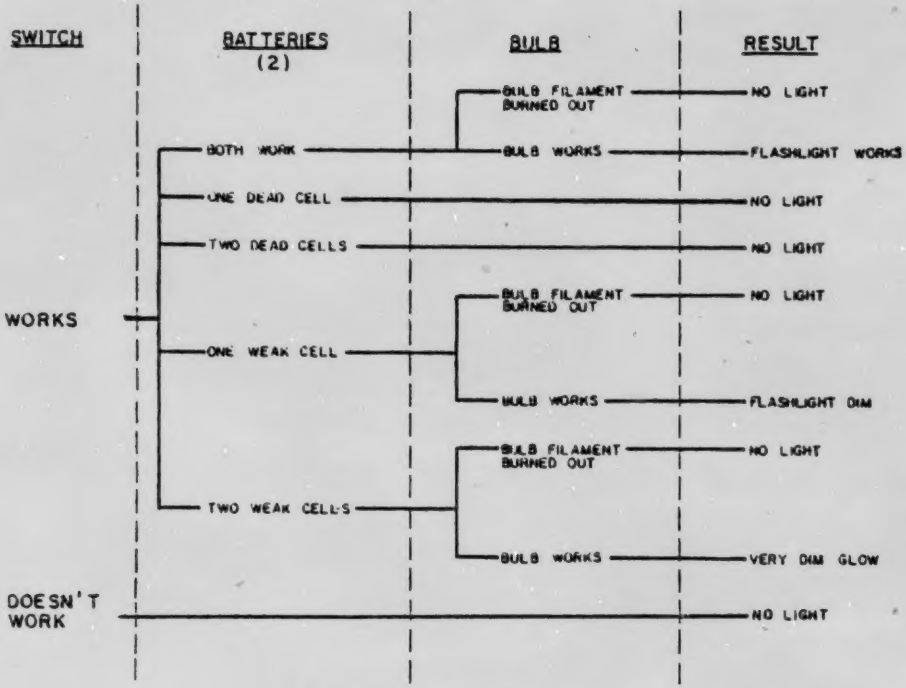

SWITCH
BATTERIES (2)
BULB
RESULT
BULB FILAMENT BURNED OUT
NO LIGHT
BOTH WORK
BULB WORKS
FLASHLIGHT WORKS
ONE DEAD CELL
NO LIGHT
TWO DEAD CELLS
NO LIGHT
BULB FILAMENT BURNED OUT
NO LIGHT
WORKS
ONE WEAK CELL
BULB WORKS
FLASHLIGHT DIM
BULB FILAMENT BURNED OUT
NO LIGHT
TWO WEAK CELLS
BULB WORKS
VERY DIM GLOW
DOESN'T WORK
NO LIGHT

Figure 8-1-5. Simple event-tree/fault-tree analysis.

These components are listed across the top, and the working and nonworking capabilities are tabulated under each component for analysis. (Case, glass and contact malfunctions are ignored to make the analysis simple and instructive.)

Each simple work/not-work system or pathway can be assigned a probability based on the probabilities of the individual events making up the pathway.

The combined probability of two or more unrelated independent events is merely the product of their individual probabilities [$P_{(comb)} = P_1 \times P_2$].

If the probability of either cell being dead is 0.1 (10%), then the probability of having a flashlight with both cells being dead is 0.1 x 0.1 = 0.01 (1%); however, the probability of failure due to a single dead cell is 0.1 - 0.01 = 0.09 (9%).

The simple flashlight system can be extended in many ways. For example, there are more causes for bulb failure than a burned out filament. These include inadequate contact, broken glass envelope, no grounding, dirty glass envelope, and so on. If each of these is included, even though their probabilities are low, the fault tree becomes more complex.

The basic conclusion of the Rasmussen Report was that potential reactor accident risks are small when compared with other risks in everyday life, including the risks from natural (i.e., non-manmade) hazards (Figure 8-1-6).

The obvious conclusion is that reactors are among the safest of all human technological enterprises. Note that the scale in this figure is logarithmic, and that the probability of a fatality from an accident as a result of 100 nuclear power plants operating is about the same as the probability of being killed by a meteorite.

Latent health effects (hidden health problems that show up after a period of time) and property and injury damage probabilities (Figure 8-1-7 and Table 8-1-2), point to a conclusion that nuclear power reactors do not pose a particularly great risk. Indeed, according to the Rasmussen Report, the probability of a core meltdown is 5×10^{-5} per reactor-year, or about once in 20,000 reactor-years of operation.

The draft and final versions of WASH-1400 have been

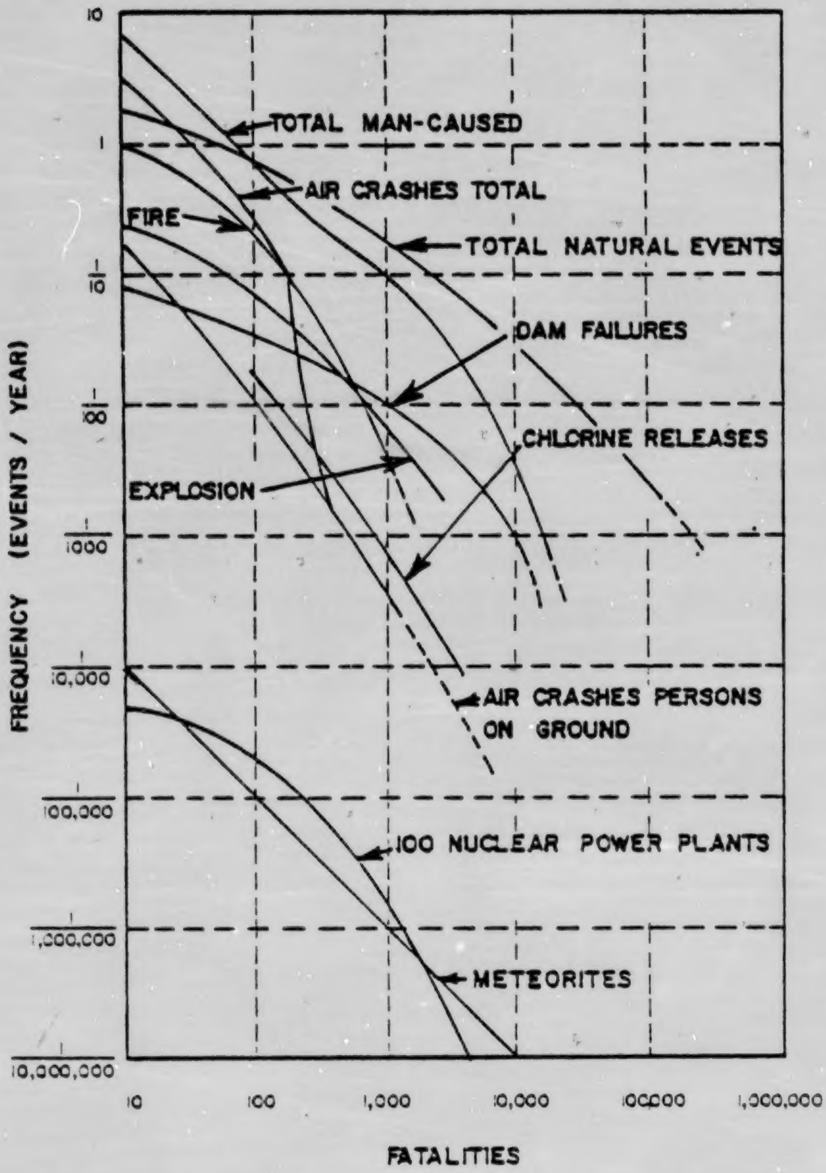


Figure 8-1-6. Worldwide frequency of fatalities from natural and man-caused events, excluding automobile accidents. (Adapted from WASH-1400.)

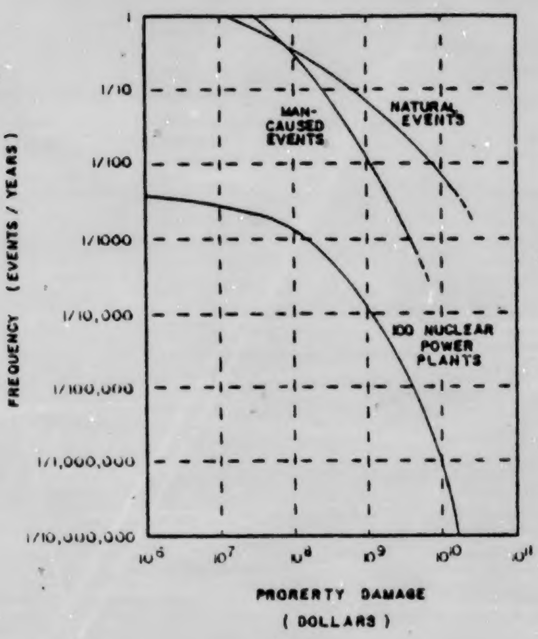


Figure 8-1-7. Frequency of property damage from reactors, other man-caused events (excluding automobile accidents), and natural events. (Adapted from WASH-1400.)

TABLE 8-1-2

INCIDENCE PER YEAR OF LATENT HEALTH EFFECTS FOLLOWING A POTENTIAL REACTOR ACCIDENT

Health Effect (per year)	Chance per Reactor per Year		Normal Incidence Rate in Exposed Population (per year)
	One in 20,000	One in 1,000,000	
Latent Cancers	< 1	170	17,000
Thyroid Illness	< 1	1400	8,000
Genetic Effects	< 1	25	8,000

Rates caused by reactor accidents are temporary and decrease with time. The bulk of cancers and thyroid nodules occur over a few decades, and the genetic effects become significantly reduced in five generations.
(Adapted from WASH-1400.)

criticized, both with regard to results and techniques used; however, the basic conclusion remains the same (unless vastly different results are obtained or the societal outlook or definition of risk is extensively altered).

The most searching and detailed evaluation of the draft version of WASH-1400 was done by a special study group of the American Physical Society. This latter group questioned the effectiveness or validity of the methods used, noting the difficulty of accurately quantifying probabilities of such rare events. Their own calculations of biological and long-term land effects were significantly greater than WASH-1400, but not sufficiently greater to alter the basic findings or conclusions of the Rasmussen Report.

EXERCISES

1. Determine the probability of reactor emergency system not receiving power (given Figure 8-1-3 and the following probabilities and conditions):

   Reactor shutdown.

   Probability of outside power sources being unavailable = 0.05.

   Probability of emergency diesel electric starter not functioning = 0.02.

   Probability of emergency diesel compressed air starter not functioning = 0.02.

   Probability of one diesel malfunctioning after starter signal received = 0.01.

2. By using the graph in Figure 8-1-6, determine yearly frequency of the following:

   Dam failure causing 1000 deaths.
   Meteorite causing 10 deaths.
   Accident in nuclear power plant causing 100 deaths.
   Airplane crash causing 100 deaths.

3. Find one example of a redundant safety system in each of the following:

   An automobile.
   An airplane.
   A reactor.

4. List the simple sequence of events leading to a DBA.
5. Show, with the aid of an event tree, at least three different possibilities following the accidental dropping of a spent-fuel element.

MATERIALS

None.

PROCEDURES

1. Locate the closest nuclear reactor. (Utility owned power reactor is preferred, but, if it is not avail-

able, a university research reactor will suffice.)

2. Write a letter to the plant manager, explaining your student project, and request permission to visit the facility to meet with the manager and/or safety supervisor. (Use Program Chairman's knowledge of nuclear facility personnel to help you obtain access.)
3. Visit plant. The objective is to obtain sufficient general information about safety protection devices and safety responsibility assignments to be able to write a minimum three-page report covering at least the following:
    - Name of plant, its location and date of start of power operation.
    - Plant owner, name of plant manager, and safety supervisor.
    - General description of their safety plan and responsibilities for plant safety.
    - List and description of at least two redundant and two multiple safety devices they have installed.
    - Description, in your view, of their philosophy and attitude toward safety.

DATA TABLE

None.

REFERENCE MATERIALS

Lawson, C.G. "Emergency Core Cooling Systems for Light Water Cooled Power Reactors." USAEC Report ORNL-NSIC-24 (1968).

Available by writing Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

Murray, Raymond L. *Nuclear Energy*. New York: Pergamon Press, 1975.

See especially Chapter 20, pp. 188-200.

"Report to the American Physical Society by the Study Group on Light Water Reactor Safety." *Review of Modern Physics* 47, Supplement 1 (Summer 1975).

Thompson, T.J. and Beckerley, J.G. *The Technology of Nuclear Reactor Safety*, 2 Vols. Cambridge, MA: MIT Press, 1964.

U.S. Atomic Energy Commission. "The Safety of Nuclear Power Reactors and Related Facilities." Report WASH-1250, July 1973.

U.S. Nuclear Regulatory Commission. Title 10 - Atomic Energy, *Code of Federal Regulations*, Part 50.

________. "Reactor Safety Study (The Rasmussen Report)." WASH-1400, October 1975.

Government documents available by writing Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

1. Directions: Listed below are several nuclear plant components and terms. You are to classify these according to the three main criteria of basic reactor safety philosophy; therefore, place 1, 2 or 3 in the blank space in front of the term (as coded below):

   Code 1 means an inherently safe design criteria.
   Code 2 means a multiple barrier criteria.
   Code 3 means a multiple and redundant safety systems criteria.

   ________ $(-\Delta T/k)$.
   ________ Reactor vessel.
   ________ Safety-rod electromagnets.
   ________ Control-rod systems.
   ________ Fuel cladding.
   ________ Containment vessel.
   ________ Control-rod fall by gravity.
   ________ Safety injection system.
   ________ Reactor fuel.
   ________ ECCS.

2. Explain each of the three criteria incorporated in basic safety philosophy:

3. Directions: Listed on the right below are words used in nuclear safety terminology. You are to match these words with the description given on the lefthand side

by placing the appropriate letter in the blank space in front of the description on the left (USE EACH LETTER ONCE ONLY):

(1) _____Application of three levels of safety.

(2) _____A mandatory organization to ensure the adequacy of records, documentation and retrievability.

(3) _____Science devoted to the weather and its relationship to reactor siting.

(4) _____Area in which an individual would receive a whole body dose of 2.5 rem.

(5) _____Report issued in Oct., 1975, called WASH-1400.

(6) _____Class 8 classification of postulated accidents.

a. DBA
b. Exclusion area.
c. LOCA.
d. Quality assurance.
e. Reactor Safety Study (Rasmussen Report).
f. Defense-in-depth.
g. Low-population zone.
h. Quality control.
i. Meteorology.
j. Population center distance.

4. Directions: Implementation of a safety program requires three levels of safety to be applied in the design phase. Listed below are five statements; assign a safety level to each by placing 1 in the blank space to the left if it is a first-level category, 2 if it is second-level and 3 if it is third-level.

_____"Additional safety systems must be included to protect the public and operators."

_____"Based on the evaluation of postulated accidents."

_____"Based upon maxiumum safety during normal operations."

_____ "Safety levels that consider major or catastrophic natural events."

_____ "Incorporation of high quality standards and engineering practices."

5. From Table 8-1-1, "Classification of Postulated Accidents," briefly explain the meaning of each accident class (1 through 9); explain basic differences between adjacent classes 4 and 5, 7 and 8, and 8 and 9.

6. List effect on environment of four potential hazards associated with postulated accidents:

(1)

(2)

(3)

(4)

7. From information on the Rasmussen Report (given in this module) state your understanding of each of the following:

   Purpose.

   Method used for analysis.

   Major items of conclusion.

   General impact on nuclear industry.

8. Sketch a simple event-tree/fault-tree for a butane cigarette lighter; show the following major elements, and functional and nonfunctional modes:

   Striker.   Gas (fuel).   Case.
   Flint.   Wick.

SUPER TOUGHIES!

9. Calculate the total probability of a reactor containment vessel rupture if the following independent probabilities exist and any one of the listed items leads to a rupture:

   Seismic event, 0.005.
   Weld fault, 0.01.
   Metal plate failure, 0.007.
   Overpressure, 0.002.

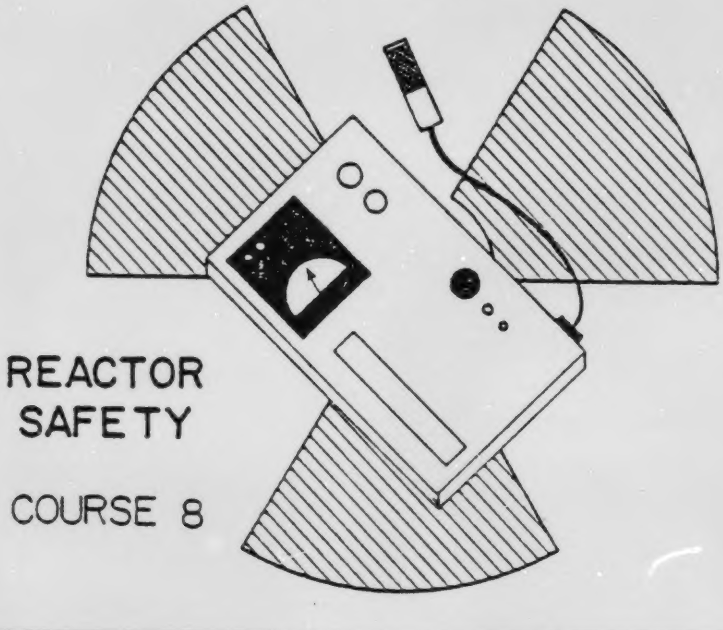
   Express your answer in 10^x units.

10. Calculate total probability of a rupture if (2) and (3) above only lead to a rupture, and (4) takes place first:

NUCLEAR TECHNOLOGY

MODULE 8-2 REACTOR LICENSING. -

RONALD L. KATHREN
PORTLAND GENERAL ELECTRIC COMPANY


REACTOR
SAFETY
COURSE 8

TERC-SW

TECHNICAL EDUCATION RESEARCH CENTER — SOUTHWEST
4201 LAKE SHORE DRIVE WACO, TEXAS

COURSE MODULES

COURSE 8. REACTOR SAFETY

	MODULE 8-1	Introduction to Reactor Safety
⇨	MODULE 8-2	Reactor Licensing
	MODULE 8-3	Reactor Protection Systems
	MODULE 8-4	Reactor Emergency Systems
	MODULE 8-5	Safeguards and Security

Copyright in 1977 by the Technical Education Research Center, Inc. Printed in the United States of America. All rights reserved. These materials, or parts thereof, may not be reproduced in any form without permission.

The materials contained herein were developed pursuant to a contract with the Office of Education, U.S. Department of Health, Education and Welfare: Contract No. 300760356. Contractors undertaking such projects under Government sponsorship are encouraged to express freely their professional judgment in the conduct of the project. Points of view or opinions stated do not, therefore, necessarily represent official Office of Education position or policy.

Technical Education Research Center
Southwest
4201 Lake Shore Drive, Suite 111
Waco, Texas 76710

INTRODUCTION

According to the dictionary, a license is a permit or permission to carry on (or be excused from) certain activities, granted by an official body. Thus, the granting of a license may allow a person to engage in certain business activities, practice a trade or profession, operate a radio-telephone, drive an automobile or even own a dog.

Licensing accomplishes several purposes, including raising revenue for the state (e.g., motor vehicle licenses, business licenses), limiting the number/location of certain types of businesses to maintain earnings and provide economic protection to the licensees. Most importantly, however, it protects public health, safety and welfare. Thus, drivers are licensed after first demonstrating their knowledge of motor vehicle laws and their ability to safely operate and control a vehicle. Physicians, dentists, engineers, electricians and pest-control operators are licensed after having demonstrated to a knowledgeable group - the professional licensing board - that they are qualified and competent to practice their profession without endangering public health and safety.

For the protection of the public health and safety, various structures and types of operations are also licensed. Elevators are granted licenses based on their ability to operate safely; nursing homes, hospitals and many other types of businesses are similarly licensed after having demonstrated that they comply with proscribed laws and regulations.

So too, are reactors licensed; but the reactor licensing process is far more complex, lengthy and difficult procedure than most other licensing operations. This module provides an examination of the reactor licensing process, including documentation requirements and the philosophical/legal bases underlying it.

A brief discussion of reactor operator licensure is also included.

MODULE PREREQUISITES

The student should have a basic understanding of reactor operations and design, radiation protection and radiation physics as might be obtained by completion of Course 1, "Radiation Physics," Course 2, "Radiation Protection," Course 5, "Introduction to Nuclear Systems," and Course 7, "Reactor Operations." In addition, the student should have completed the previous module in this Course (Module 8-1, "Introduction to Reactor Safety").

OBJECTIVES

Upon completion of this module, the student should be able to:

1. Explain the legal basis of reactor licensing process.
2. State purpose and general content of a Safety Analysis Report.

3. State purpose and general content of an Environmental Report.
4. Explain why it is important that nuclear facility personnel be familiar with its Safety Analysis Report.
5. Explain importance of facility and component design to safety.
6. Explain relationships between Safety Analysis Report, Environmental Report and other licensing documents.
7. Differentiate between requirements for a reactor operator and a senior reactor operator.
8. Define:
    - License.
    - Law.
    - Rule.
    - Regulation.
    - Regulatory Guide.
    - Environmental technical specification (ETS).
    - Safety technical specification (STS).
9. Trace flow of a Safety Analysis Report and an Environmental Report for a nuclear power plant.

stated that licenses could only be issued if adequate measures had been included for protection of the public health and safety.

To carry out its charges of licensure, regulation and protection of the public health and safety, AEC was given broad regulatory and rule-making authority. The entire title (Title 10 of the Code of Federal Regulations) was set aside for AEC; over the years, extensive regulations relating to nuclear power have evolved.

Regulations and laws differ in how they are brought about, although their net effect may be the same. Laws are products of elected legislative bodies, such as Congress or a state legislature, and are generally broadly worded. For passage, a Federal law may first go through a political process in both houses of Congress, followed by approval (signing) by the President. In matters such as atomic energy, which are highly complex and require a great deal of specialized expertise, legislative bodies often produce a law that lays down a framework of what it wishes done and creates an administrative body to carry out the legislative intent. Such laws are often known as "enabling legislation," since they permit another body to carry out certain broad functions, including regulatory functions.

The Atomic Energy Commission was a regulatory body. (Examples of other regulatory bodies include the Interstate Commerce Commission, the Federal Power Commission and the Federal Communications Commission.) Such bodies or commissions exercise the three principal functions of government:

Administrative (executive).
Legislative.
Judicial.

LEGAL AND PHILOSOPHICAL OVERVIEW:
ATOMIC ENERGY COMMISSION

In 1946, a scant year after the conclusion of World War II, control over the development of atomic energy was transferred from the military to a civilian agency - the newly created Atomic Energy Commission (AEC). This five-member body was charged, not only with development of nuclear energy, but also with protection of public health and safety.

Since, at the time, the Federal Government was, by law, the sole owner of all fissionable materials and related facilities (including the gaseous diffusion plant at Oak Ridge, plutonium production reactors and chemical separation plant at Hanford and several laboratories for research), AEC had a monopoly over atomic energy development and use. Private activities were restricted to those performed under contract with the Federal Government.

Eight years later, in 1954, a new Atomic Energy Act became law and ended the Federal monopoly. It opened to private industry and individuals an opportunity to participate in development and use of this new technology. Participation was tempered, however, by a comprehensive Federal licensing act and by regulatory programs administered by AEC. (AEC retained a monopoly on nuclear weapons.) Even so, widespread participation led to scientific and industrial progress in development and use of atomic energy for peaceful purposes.

The Act provided for a variety of licenses, including those for nuclear power reactors. Also, it specifically

In the legislative area, AEC delivered a series of regulations to carry out the broadly phrased enabling legislation passed by Congress and signed by the President. Thus, a regulation is a rule or order put forth by an appointed body created for a specific purpose (in this case, the safe implementation of nuclear power).

Regulations have the weight of law but are generally more easily and quickly passed and put into force. They are also much more detailed and specific. And, although passed by an appointed body, they have the same force of law as the statute that empowered the appointed body that creates them. (The enabling statute, while broad, does establish the general area of authority for the regulatory body. AEC, for example, could not pass regulations pertaining to agricultural commodities or harbors unless somehow these were an integral part of the atomic energy program.)

In addition to forming regulations, AEC acted in an administrative capacity, watching over and enforcing the observance of statutes (laws), rules, regulations and judicial findings and conducting investigations and studies of various matters affecting their assigned areas. An important area pertains to rule-making. A rule is a requirement, imposed on the Commission or its staff, which ordinarily pertains to conduct of its operations. Rules effectively have the same force as laws or regulations and, in many cases, are included in the regulations.

Another administrative function of AEC was licensing, which was carried out in a semi-judicial fashion through the mechanism of a formal hearing. (Commissions can also issue orders, which are usually specific, resembling a court order.)

In the strict judicial area, AEC could and did function as a court, having the power to hold hearings and judge cases involving alleged infractions of regulations. Decisions reached by these actions, which may have included assessments of fines or revocations or denials of licenses, were enforced in much the same manner as are procedures in the courts.

By law (Administrative Procedures Act), every commission or regulatory body must publicize the methods and procedures by which it works, and it must specify how individuals can bring proposals and requests before it. When considering a new rule or regulation (or change to an existing one), the commission must give ample notice to all concerned; this is normally done by publication of the proposed action in the Federal Register. In addition, hearings must be held to provide for public input. Commissions also are empowered to serve subpoenas and to take sworn testimony.

Since no five-member body could hope to carry out the functions imposed on by the Atomic Energy Act of 1954, AEC was provided a staff. Through their efforts, a comprehensive set of regulations for overseeing the development, licensing and safety of nuclear power plants specifically, and atomic energy generally, was established.

OVERVIEW: NUCLEAR REGULATORY COMMISSION

The Energy Reorganization Act of 1974 abolished AEC, transferring most of its development and research functions to a newly created Energy Research and Development Administration (ERDA). The regulatory and licensing functions were transferred to another new agency - the Nuclear Regulatory Commission (NRC) - which inherited the regulations established by AEC.

The 1974 law specifically charged NRC with certain regulatory activities that were only hinted at in the 1954 Atomic Energy Act. NRC's Office of Nuclear Reactor Regulation was established to review reactor safety systems and evaluate transportation and storage of radioactive wastes and special nuclear material. An Office of Nuclear Material Safety and Safeguards provided for safeguards against theft, threats and sabotage of facilities and materials licensed by NRC. Each year, NRC must report its activities and findings in these specific areas as well as others.

In 1977, all Federal energy activities except NRC were incorporated into a single Department of Energy (DOE); however, NRC remained an independent regulatory agency, essentially unchanged in purpose or authority.

CODE OF FEDERAL REGULATIONS

The Code of Federal Regulations contains rules and regulations adopted and enforced by NRC. This Code has 50 titles (or sections); Title 10 relates to energy. Title 10 contains one chapter - "Nuclear Regulatory Commission" - which is divided into 45 parts and covers specific regulatory areas. Listed in Table 8-2-1 are the parts of Title 10 that deal primarily with reactor licensing and safety. These 14 parts include over half of the nearly 600 pages of regulations.

In addition to the regulations published in Title 10, NRC issues almost continuous Regulatory Guides. These guides include methods and procedures the NRC staff finds accept-

TABLE 8-2-1

PORTIONS OF TITLE 10, CODE OF FEDERAL REGULATIONS PRIMARILY RELATED TO REACTOR SAFETY AND LICENSING

PART	NAME	COMMENT
1	Statement of Organization and General Information	Describes the organization of the NRC
2	Rules of Practice	Governs the conduct of proceedings for granting, revoking, amending, or taking other actions regarding NRC licenses; civil fines; rulemaking procedures; patent matters
9	Public Records	Identifies and governs the availability of public records, including licensing documents
19	Notices, Instructions, and Reports to Workers; Inspections	Includes reporting radiation exposure data to work and provides procedure for inspection of licensees
20	Standards for Protection Against Radiation	Establishes standards and regulations for protection against radiation
50	Licensing of Production and Utilization Facilities	Gives the requirements for obtaining a construction permit or operating license for a reactor, including a detailed account of the information which must be supplied by an applicant for such a permit or license, and design safety criteria
51	Licensing and Regulatory Policy and Procedures for Environmental Protection	Gives the procedures to be followed by an applicant for NRC license to satisfy the National Environmental Policy Act
55	Operators' Licenses	Gives procedures and criteria for the issuance of licenses to operators of NRC - licensed reactor facilities
70	Special Nuclear Material	Establishes regulations and criteria for the issuance of licenses to own and use special nuclear material (roughly speaking, any fissile material or uranium enriched in ^{235}U)
71	Packaging or Radioactive Materials for Transport and Transportation of Radioactive Materials Under Certain Conditions	Gives license requirements for shipment of fuels and requirements for shipping containers
73	Physical Protection of Plants and Materials	Covers requirements for safeguarding SNM in transit or at fixed sites
100	Reactor Site Criteria	Defines and describes site suitability criteria and evaluation on basis of safety
115	Procedures for Review of Certain Nuclear Reactors Exempted from Licensing Requirements	Establishes method for safety review of NRC owned reactors; parallels Parts 2, 50 and 55
140	Financial Protection Requirements and Indemnity Agreements	Gives liability and financial requirements for licensees and methods of determining liability and indemnification

able or suitable for meeting its regulations; they also provide specific techniques used by the NRC staff in evaluating reactor license applications. The guides are issued in ten broad divisions:

Power reactors.
Research and test reactors.
Fuels and material facilities.
Environmental and siting.
Materials and plant protection.
Products.
Transportation.
Occupational health.
Anti-trust review.
General.

Although the guides are not part of the regulations (it is not mandatory for an applicant to follow them), they have assumed an increasingly important role and are often accepted by license applicants as if their requirements were, in fact, mandatory.

STATE AUTHORITY OVER REACTORS

Although some states have passed legislation designed to regulate (or otherwise control) siting, construction and operation of nuclear power reactors, there remains the question of whether the states can rightfully enter into the field of reactor regulation and licensing. The Atomic Energy Act of 1954 clearly delegated this responsibility to AEC (now NRC); one section of the Act, passed as an amendment in 1959, specifically forbids the yielding of this power to other authority. In 1971, the State of Minnesota attempted to impose more stringent requirements on radioactive emissions from a nuclear power plant. The case, Northern States Power Company versus Minnesota, was decided by the Supreme Court, which held that Federal legislation had pre-empted this area of regulation.

Still, many states have passed legislation and implemented mechanisms that do, in fact, regulate some aspects of nuclear reactors. A few, such as New York and Maryland, have signed what are known as "274 agreements," stating their intention to abstain from regulatory areas pertaining to radiological hazards. Maryland, on the other hand, has a siting law that requires the state to select, and hence approve, sites for nuclear power plants; however, regulation is not a feature of that law.

Other states have various siting requirements that, to a greater or lesser degree, control or regulate nuclear reactor locations and operations. While these requirements use zoning or nonradiological considerations as their basis, the underlying factor is essentially one of safety. State regulation for purposes other than protection against radiation hazards is apparently possible if not permissible under the Atomic Energy Act of 1954.

Many states - California, Washington, Maryland, New York, Colorado, Minnesota, Vermont and Oregon, most notably - have regulatory requirements directly affecting nuclear reactors. In Vermont, approval of both houses of the legislature is required before the Vermont Public Service Board can issue a "certificate of public good" permitting the construction of a nuclear power reactor. Oregon requires all reactors - even research reactors - to obtain a site certificate and has a comprehensive set of laws and regulations applicable to nuclear reactors. Washington and California provide for public hearings on siting. Most of the other states mentioned above have requirements that fall somewhat short of the comprehensive model of Oregon, but exceeding a strict hands-off approach.

As yet, the role of the states with respect to licensing of nuclear reactors is highly variable and also uncertain. Other than the Northern States Power Company versus Minnesota case in 1971, there has been little to clarify the legal questions, although there seems to be general agreement on the following two points:

Federal Government has pre-empted the states from regulating nuclear power plants on the basis of radiological hazards.

State and local agencies can regulate NRC-licensed reactors for purposes other than protection against radiological hazards.

Thus, states can and do regulate and license nuclear reactors (in addition to licensure from NRC); a reactor may be required to have numerous permits and licenses from various state, local and other federal bodies. In some cases, almost 100 such licenses and permits may be required. But, only the NRC license is based on radiological hazard and safety aspects of the facility.

INITIAL NRC LICENSING PROCEDURES

The general sequence of the NRC licensing procedure is lengthy. It begins with determination of a need for power and the site selection process. These early studies become an important part of any subsequent license application. Often, NRC is consulted for an informal review of a potential site.

CONSTRUCTION PERMIT

Once a need has been verified and an appropriate site selected, application for a construction permit (CP) is made. For a power reactor, this application includes the following documents:

- General information.
- Preliminary Safety Analysis Report.
- Environmental Report - CP stage.
- Anti-trust information.

The general information document contains the following:

- Name, address and relevant business information of the applicant, including financial statements.
- Names, addresses and citizenship of directors and officers (if a corporation) and similar data.

The Preliminary Safety Analysis Report (PSAR) is a lengthy document describing reactor design and technical and administrative bases of safety. (The PSAR is discussed in detail below.) The Environmental Report (ER) is a separate document that describes environmental impacts of the proposed reactor. The ER is used as a basis of the Environmental Impact Statement, which is prepared by NRC in accordance with the National Environmental Policy Act of 1969. (A detailed discussion of the ER process is also presented later.)

Also required for a commercial power reactor applicant is information relating to anti-trust. Ordinarily, the anti-trust portion of the application is prepared by non-technical personnel for submission to the Attorney General. Here the application is reviewed to ensure that the facility, if constructed, will not be violation of existing anti-trust laws.

APPLICATION REVIEW

After the application has been submitted, it is given a brief review by the NRC regulatory staff to determine its completeness and general conformance to regulations. Thirty days are allowed for this review. If the application passes this "mini-review," it is assigned a docket number before undergoing a thorough review by the NRC staff and others, a process which may take up to eighteen months. During this review, the applicant may be asked detailed questions by the regulatory staff, and there will be a constant flow of letters between the applicant and NRC.

The license application also is reviewed by an Advisory Committee on Reactor Safeguards (ACRS). This body, which has a maximum of 15 members, was established in 1957 by an amendment to the 1954 Act. Members of the ACRS provide independent review of all power reactor license applications and report their findings directly to NRC. ACRS members, selected from the scientific and technical community, are not employees of, but rather consultants to, NRC.

The review process by the regulatory staff results in two documents:

A Safety Evaluation Report, which summarizes staff findings and conclusions, noting that the facility can (or cannot) be built without undue risk to public health and safety.

A draft Environmental Statement, which summarizes results of staff findings relating to environmental impacts, including need for the power to be generated by the reactor. This draft document is circulated to various agencies, organizations and individuals for comments; then a Final Environmental Statement is prepared.

A third document issued by the staff is the Supplemental Safety Evaluation Report, which is based on PSAR reviews by the ACRS. It includes any safety concerns raised by the ACRS, as well as any new information (relating to safety) that may have been obtained after the Safety Evaluation Report was prepared. The ACRS also reports its findings in a summary document sent to the NRC chairperson.

After these documents have been issued, a public hearing is held before the Atomic Safety and Licensing Board (ASLB) convened for that purpose. This three-member body is generally headed by an attorney or hearings officer, who serves as chairperson, and two technically qualified members - usually one scientist and one engineer. The hearing, held at a location near the proposed site, is in two parts:

Environmental hearing.
Safety hearing.

The Atomic Energy Act of 1954 permits anyone whose interests may be affected by the proposed plant to intervene and become a party to the proceedings. Thus, some groups or individuals may intervene to halt construction or to gain certain changes relating to safety or environmental considerations. Most hearings for power reactor construction permits or licenses are contested, with testimony (and cross-examination) provided by the NRC staff, the applicant and any intervenors.

Because the process is so lengthy, a mechanism is available whereby the applicant can be issued limited work authorization (LWA). This permit allows the applicant to prepare the site for construction, perform excavations, install foundations and construct roads, railway spurs and borrow pits, and to begin other preliminary construction activities. The LWA is issued, however, only after staff review and environmental hearings lead to the conclusion that 1) the plant can be constructed without harm to the environment and 2) the site is suitable for a nuclear facility.

At the conclusion of the hearings, the ASLB considers evidence, testimony and other information presented and issues an initial decision. If the hearings are favorable and uncontested, a construction permit is issued and work can begin. If the hearings have been contested, the construction permit may be issued (as required by regulations), but the intervenors may file exceptions and appeal the decision of the ASLB. Similarly, any party - staff, applicant or intervenor - to the proceedings can file an appeal if dissatisfied with the ASLB decision.

Appeals are heard by an Atomic Safety and Licensing Appeals Board (ASLAB), which considers only those matters brought before it. The ASLAB will not consider the entire matter again, only specific exceptions/contentions of error in law or fact. Decisions of the ASLAB can be appealed also - directly to the Commission (NRC). If the party is still not satisfied with the decision, as made by NRC, the matter can be taken before a Federal court, and progress as far as the U.S. Supreme Court.

OPERATING LICENSE

A similar procedure is followed at the operating license (OL) stage, which begins about one-third of the way through construction. A Final Safety Report (FSR) and an Environmental Report - OL stage - are filed and reviewed by the regulatory staff and the ACRS.

These reviews are quite thorough and emphasize any new information or data that may affect safety or environmental considerations of the plant. Since the design, as well as operating organization, will have been made firm, these areas are perhaps more carefully considered. In any event, the regulatory staff issues a "new" Safety Evaluation Report and draft Environmental Statement. The ACRS also makes a second independent review, again reporting its findings in a letter to the NRC chairperson.

Although a hearing regarding safety is not mandatory at the OL stage, one is ordinarily held if there is substantial public interest or a petition to intervene or, possibly, significant changes in the facility as originally planned. The ASLB procedure and the appeal process are virtually identical to that described for the CP stage.

For power reactors, the licensing-construction procedure (Figure 8-2-1) takes about ten years, with delays (from the applicant's point of view) occurring from questions and legal maneuvers by intervenors, labor difficulties (strikes) and regulatory changes. Even if there were no licensing, however, construction alone would take from four to five years, assuming no labor or material shortages or other problems.

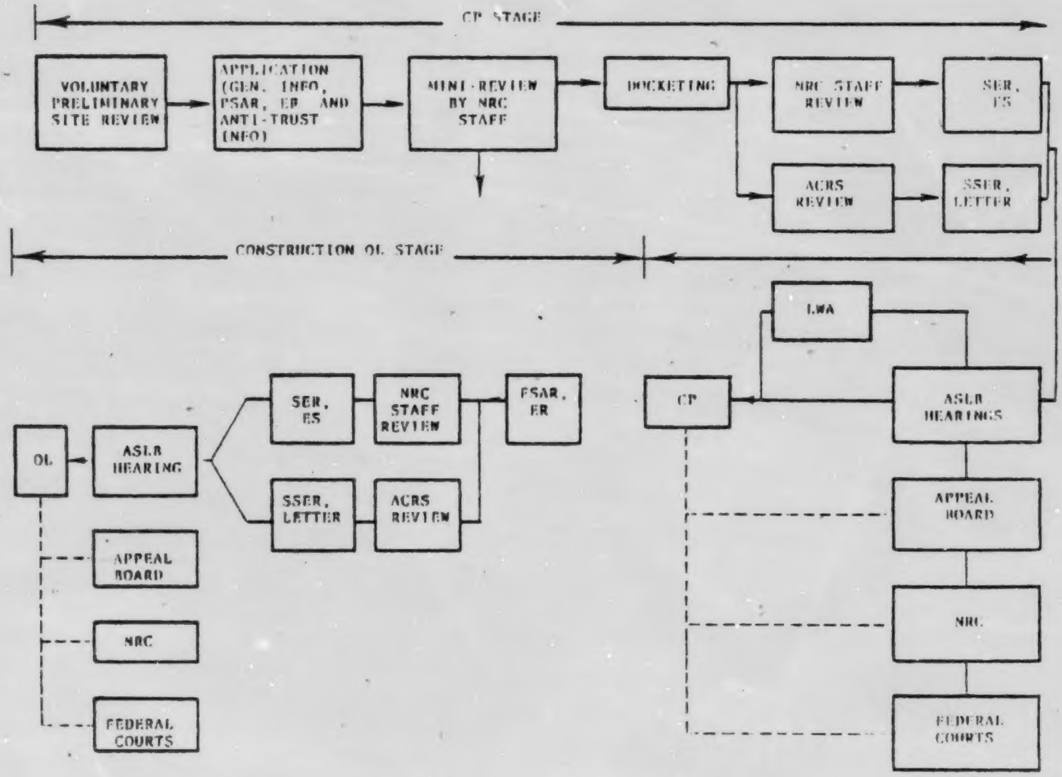

CP STAGE
VOLUNTARY PRELIMINARY SITE REVIEW
APPLICATION (GEN. INFO, PSAR, ER AND ANTI-TRUST INFO)
MINI-REVIEW BY NRC STAFF
DOCKETING
NRC STAFF REVIEW
SER, ES
ACRS REVIEW
SSER, LETTER
CONSTRUCTION OL STAGE
LWA
CP
ASLB HEARINGS
APPEAL BOARD
NRC
FEDERAL COURTS
OL
ASLB HEARING
SER, ES
NRC STAFF REVIEW
FSAR, ER
SSER, LETTER
ACRS REVIEW
APPEAL BOARD
NRC
FEDERAL COURTS

Figure 8-2-1. Flow chart showing licensing path for nuclear power reactor.

Two kinds of licenses are issued by NRC for reactors:

Class 104 licenses are issued to reactors used for research and development purposes, or for medical therapy; an anti-trust review is not required.

Class 103 licenses are issued to commercial power reactors.

The first Class 103 license, bearing number NPF-1, was issued for the Trojan Nuclear Plant (a 1130-MWe PWR), operated by Portland General Electric Company at a site about 40 miles north of Portland, Oregon, on November 21, 1975. Prior to this, all power reactors were issued Class 104 licenses, leading to the comment by some opponents of nuclear power that these were, in fact, experimental reactors.

The licensing process is a lengthy and expensive one, paid for, to a great extent, by licensing fees (Table 8-2-2);

TABLE 8-2-2
FEE SCHEDULE FOR REACTOR LICENSING

REACTOR TYPE	CP APPLICATION FEE	CP ISSUE FEE	OL APPLICATION FEE	ANNUAL OL FEE
POWER REACTOR	$125,000	$250,000+ $170/MW(t)	$250,000+ $170/MW(t)	$65/MW(t)*
TESTING REACTOR	3,900	10,500	15,200	13,000
RESEARCH REACTOR	600	2,300	3,500	8,500

*$20,000 minimum yearly fee

non-profit, educational institutions and government agencies are fee-exempt, except for power reactors. The licensing fee for a 1000 MWe reactor operating at 33% net efficiency [which requires 3000 MW(t)] is calculated as follows:

CP application	$ 125,000
CP issue	760,000
OL application	805,000
Total	$1,690,000

plus an annual operating license fee of $195,000.

SAFETY ANALYSIS REPORT

Every reactor, regardless of size, use or fee requirements, is required by Part 50 of the regulations to submit a Preliminary Safety Analysis Report (PSAR) as part of its construction permit application, and a Final Safety Report (FSR) as part of its application for an operating license. Size and content of these reports depend on size and complexity of the reactor. Thus, a PSAR for a small research or teaching reactor may run to a few hundred pages, while a PSAR for a large power reactor may be several thousand - perhaps 20,000 to 30,000 - pages long and include hundreds of tables, illustrations and calculations.

Contents of a PSAR can be gained from examination of the 17 chapter headings specified for light-water power reactor safety analysis reports (Table 8-2-3).

The first chapter provides an overview of the plant and some details regarding reference materials and drawings. The second chapter details the site, including in-depth consideration of geography, industry and population characteristics (and projections for 50 years), as well as meteorology, hydrology, geology and seismology of the site. This chapter receives major consideration in the granting of a LWA.

Most of the remaining chapters deal with specifics of design, safety systems and effects of hypothetical accidents. A major consideration is Chapter 3 (relating to design), which considers ability of the reactor to withstand effects of various maximum natural disasters (i.e., earthquakes, flooding, tornadoes and other wind loadings) and missiles (as might be produced from explosions or turbine breakup).

TABLE 8-2-3
SAR CHAPTER HEADINGS

CHAPTER	TITLE
1	Introduction and General Description of Plant
2	Site Characteristics
3	Design of Structures, Components, Equipment and Systems
4	Reactor
5	Reactor Coolant System and Connected Systems
6	Engineered Safety Systems
7	Instrumentation and Controls
8	Electric Power
9	Auxiliary Systems
10	Steam and Power Conversion System
11	Radioactive Waste Management
12	Radiation Protection
13	Conduct of Operations
14	Initial Tests Program
15	Accident Analyses
16	Technical Specifications
17	Quality Assurance

Particular attention is given to analysis of seismic events; a listing is provided of structures, systems and components important to reactor safety that must remain functional in event of "Safe Shutdown Earthquake." Such structures and components, designated "Seismic Category I," include all plant features, their supports and their foundations necessary to:

Maintain integrity of reactor coolant pressure boundary.

Provide and maintain safe shutdown.

Prevent escape of radioactivity such that off-site radiation exposures cannot exceed levels established by regulations.

Chapters 4 through 11 are primarily "hardware" chapters, essentially concerned with reactor design and operating parameters. It is in this portion of a PSAR that nuclear design parameters are given, including characterization of fuel, and reactivity controls.

Although all chapters are concerned with safety, two chapters are particularly relevant: "Engineered Safeguards" and "Radioactive Waste Management." The former considers materials used in the reactor as well as emergency cooling systems, containment and radioactivity removal and control systems. It also considers design failure analyses and inspection of individual components important to safety.

The latter chapter ("Radioactive Waste Management") presents detailed descriptions of equipment and methods for management of gaseous, liquid and solid wastes. Included is a description of all effluent monitoring equipment for radioactivity (details relating to calibration, sensitivity, accuracy, reliability and redundancy). The bases for system design are given, including anticipated system operation in an accident.

Approximately the final one-third of a PSAR is devoted to organization, operations and procedures. Included in this portion of the document is a description of the applicant's administrative organization with the names, positions, responsibilities and qualifications of key personnel. The

PSAR also may include data on the architect-engineer firm overseeing design and construction activities. Training, security, planning, and startup operations and procedures are also detailed.

An important chapter deals with "Health Physics," and includes not only the description of the company organization and personnel, but also a discussion of the equipment, personnel and facility design features provided to ensure that occupational radiation exposures are kept as low as reasonably achievable (ALARA). ALARA concepts and requirements are very important, and two Regulatory Guides (8.8 and 8.10) spell out acceptable means of ensuring minimal personnel exposures.

Also considered in the final third of a PSAR are the quality-assurance (QA) program and technical specifications. The QA section must describe the QA program generally, as well as the specifics of design control, document and drawing control, control of outside suppliers and contractors, inspections, audits, test procedures and records keeping. Records, in particular, are important, for many of these must be kept for the lifetime of the plant. A PSAR considers both QA and technical specifications during design and construction.

The safety technical specifications (STS) set forth various limits, design features, operating conditions and other requirements necessary for protection of public health and safety. These specifications are written in a special format, and include not only the specifications (e.g., specific numbers or limits on, say, heat discharge) but also the technical bases (e.g., protection of aquatic life in a receiving body) and the method of measurement or determination of compliance and references. Technical specifications, covering a wide range of operating conditions and requirements, included as appendices to the license, may run to several hundred pages in length. Those relating to safety are included as Appendix A to the operating license and, as such, are mandatory; any change to this Appendix involves license amendment, and any violations must be reported to NRC.

Under certain conditions, violations of technical specifications can result in fines or other penalties.

In addition to safety technical specifications included as Appendix A, a second, smaller set of environmental technical specifications (ETS) are included as Appendix B. These specifications deal with environmental and ecological controls; the ETS are derived from the Environmental Report and the hearing.

A final, important component of a PSAR is the chapter entitled "Accident Analyses." This chapter includes analyses of plant responses to postulated malfunctions/failures of equipment; it serves as a focal point for NRC review. In this chapter, a broad spectrum of accident-initiating events must be considered for each of eight categories:

Turbine plant heat removal increase.
Turbine plant heat removal decrease.
Reactor coolant flow rate decrease.
Unusual conditions of power distribution and reactivity.
Reactor coolant radioactivity increase.
Reactor coolant radioactivity decrease.
Radioactivity release from a subsystem or component.
Anticipated transients without scram.

Each analysis must include a summary of various plant parameters considered, as well as assumptions regarding actions of protection systems.

ENVIRONMENTAL REPORT AND IMPACT STATEMENT

In 1969, the National Environmental Policy Act (NEPA), Pulbic Law 91-190, was passed by Congress. This law required consideration of environmental consequences of any major Federal action. Further, it required responsible Federal agencies to prepare appropriate environmental impact statements, considering not only potential environmental impacts of such projects, but also possible alternatives. NEPA also required cost-benefit analyses and consideration of comments from other agencies (Federal, state and local) and the general public.

Within three months after passage of NEPA, AEC published its policy statement regarding environmental aspects of power reactor licensing. It spelled out general procedures, and contents of environmental reports and statements. AEC emphasis was on radiological aspects of reactors, with only cursory review of the nonradiological impacts.

The initial AEC interpretation was challenged in courts as being too limiting. Intervenors asserted that nonradiological issues were not fully considered, and that certain environmental issues were excluded from the licensing process if they were not raised in earlier construction permit hearings. On July 23, 1971, the U.S. Court of Appeals for the District of Columbia ruled that "... the (Atomic Energy) Commission must go further than it has in its present rules," and that "... the environmental review be as full and fruitful as possible."

This case, known as the Calvert Cliffs decision, greatly expanded the role of AEC in environmental areas. Perhaps the most significant result of the Calvert Cliffs decision was development of cost-benefit guidelines for application to power reactors. These guidelines included consideration of a whole spectrum of environmental costs, including heat and chemical discharges, noises, foggings and aesthetics. All sectors of the environment were to be considered: people, property, plants and animals.

From the Calvert Cliffs case, a comprehensive Environmental Report-Environmental Statement procedure evolved (Figure 8-2-2). This procedure parallels the safety portion of licensing and is an integral and essential part of the entire licensing action. Title 10, Code of Federal Regulations, Part 51, which deals exclusively with environmental protection, specifies the requirements for environmental documentation. Each applicant is required to submit an Environmental Report (ER), a licensing document analogous to the PSAR.

In effect, the Environmental Report is a preliminary environmental statement, subject to review by NRC, other agencies and the general public. It requires evaluation of environmental impact by the applicant and, in its 13 chapters, seeks to establish a basis for construction of the facility consistent with goals of NEPA and the Calvert Cliffs decision.

The first chapter seeks the purpose of the proposed facility, citing both the need for power and the consequences of delay. Other chapters discuss general plant design, economic and social effects of plant construction and op-

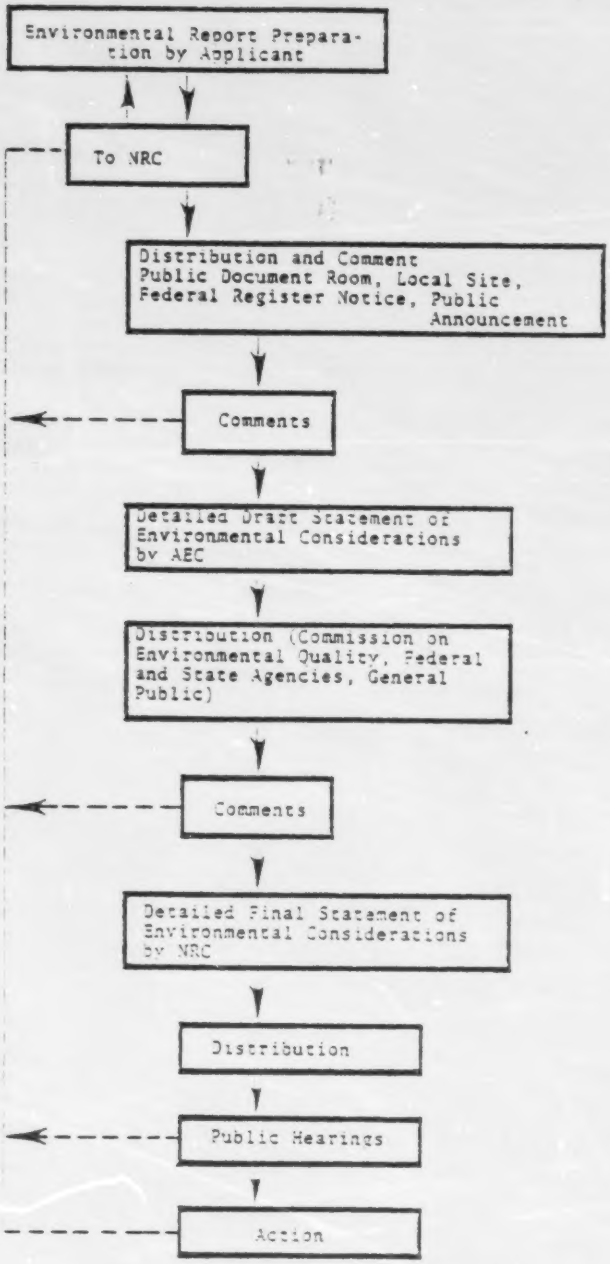

Environmental Report Preparation by Applicant
To NRC
Distribution and Comment Public Document Room, Local Site, Federal Register Notice, Public Announcement
Comments
Detailed Draft Statement of Environmental Considerations by AEC
Distribution (Commission on Environmental Quality, Federal and State Agencies, General Public)
Comments
Detailed Final Statement of Environmental Considerations by NRC
Distribution
Public Hearings
Action

Figure 8-2-2. Environmental statement preparation pathway for nuclear power plants.

eration, alternative energy sources and potential sites other than the one selected. Included in this discussion are the impact of potential tax revenues on the area, effects of temporary influx of construction workers and various other spinoff benefits or costs that may accrue to the area:

Recreational values.
Educational opportunities.
Improvement of roads or other public transportation facilities.
Beneficial or adverse effects of facility on local trade, productivity or tourism.

A major portion of the Environmental Report is devoted to hard scientific data descriptive of the site. Hydrology, geology, meteorology and ecology of the site are described on the basis of detailed and intensive original studies performed prior to operation or even construction. Much of the data, obtained from continuous pre-operational monitoring programs, will be used to establish a so-called "baseline" against which operating conditions can be compared to ensure that reactor operations have not altered pre-existent environmental conditions. Thus, meteorological, radiological and biological monitoring of the environment are all continued after plant operation, and reports of findings are sent to NRC. In addition, plant discharges of all types (chemical, thermal, radiological and sanitary) are continuously monitored, with the data collected made available to regulatory agencies.

One example of an environmental monitoring program begun pre-operationally and continued throughout the life of the plant is the radiological monitoring program. This program is designed to accomplish several purposes.

It must accurately measure the amounts and kinds of radioactivity in the environment, both from natural and human sources. Thus, waters (surface, rainfall and underground), air, soils, river or lake bottom sediments, and plants and animals are sampled and analyzed for radioactivity. The pre-operational study sets the baseline - that is, it establishes how much radioactivity was present in these media prior to startup of the reactor. These values can then be compared with others obtained after the reactor has begun operation to determine if there have been any changes due to the reactor.

A major purpose of the radiological monitoring program is to determine important exposure pathways (Figure 8-2-3) for the site. Also, it aids in prediction of radiation doses to people in the vicinity of the reactor. Hence, samples of milk, fish, game and other foodstuffs are surveyed and analyzed, and ambient doses in the environment around a potential plant site are characterized.

Another important portion of the Environmental Report is the cost-benefit analysis. Guidelines require a comprehensive comparative analysis of various plant design alternatives, including cooling systems, radioactive waste systems and transmission facilities. These are evaluated on the basis of dollar values wherever possible and summarized in a detailed comprehensive fashion.

Environmental costs are broken into a multitude of categories, further subdivided, and each analyzed. For example, no less than nine plant subsystems must be considered individually, and the impact of each on approximately 50 environmental areas (ranging from effects of salt discharge on plants and animals to raising or lowering of ground water) must be evaluated. When two or more subsystems of each type are

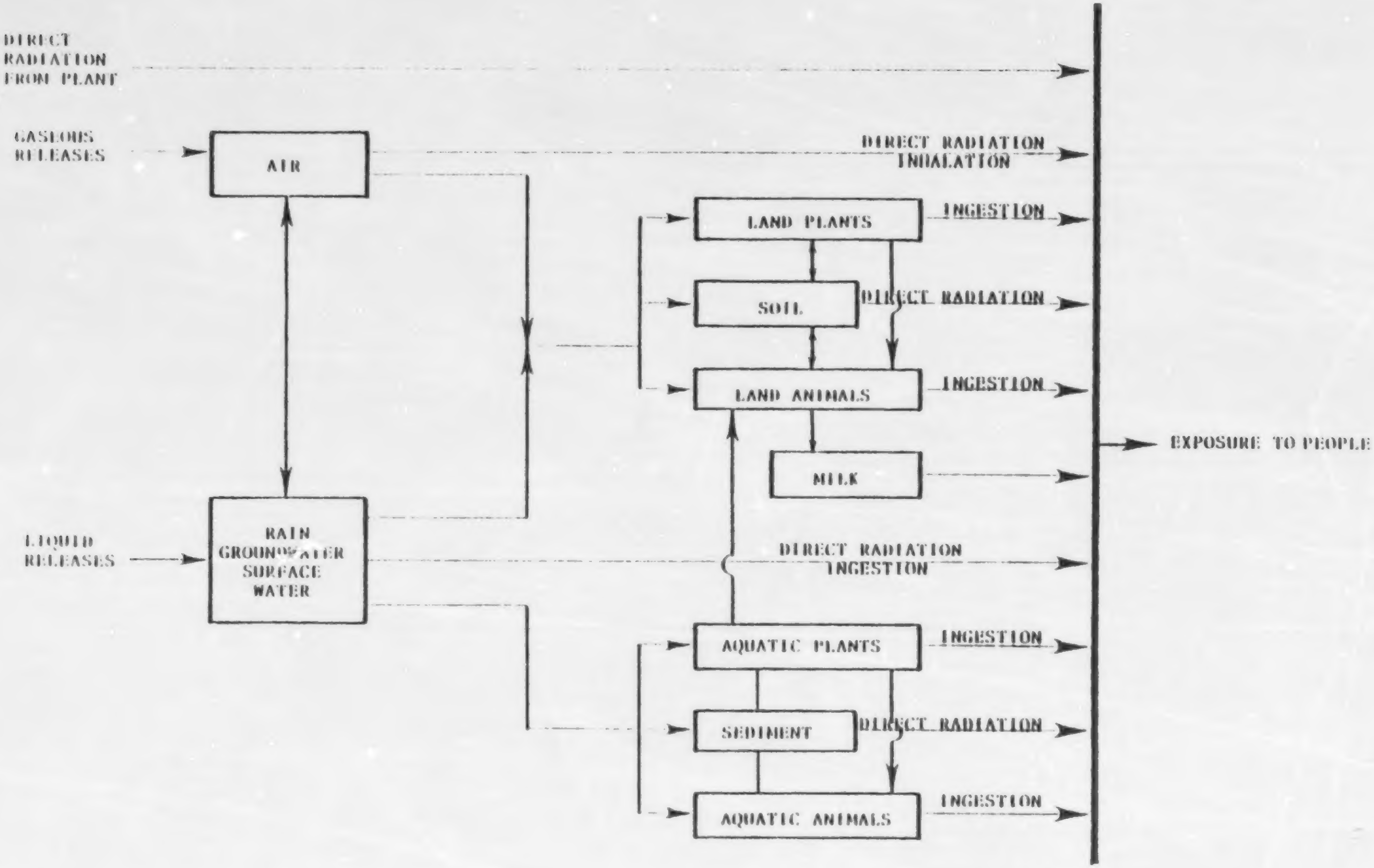

DIRECT RADIATION FROM PLANT
GASEOUS RELEASES
AIR
DIRECT RADIATION INHALATION
LAND PLANTS
INGESTION
SOIL
DIRECT RADIATION
LAND ANIMALS
INGESTION
MILK
EXPOSURE TO PEOPLE
LIQUID RELEASES
RAIN GROUNDWATER SURFACE WATER
DIRECT RADIATION INGESTION
AQUATIC PLANTS
INGESTION
SEDIMENT
DIRECT RADIATION
AQUATIC ANIMALS
INGESTION

Figure 8-2-3. Generalized radiation exposure pathways for liquid, gaseous and direct radiation. (Actual ecological interrelationships are far more complex than shown.)

considered, the summary cost-benefit analysis becomes complex and time consuming.

Difficulties of applying classical cost-benefit analyses are great, for many costs are not easily quantified. On occasion only qualitative assessments can be made. In particular, subjective factors, such as aesthetic considerations, potential applications of power to pollution control or crime prevention, and balancing human costs against ecological ones are extraordinarily difficult to evaluate.

OPERATORS' LICENSES

In addition to the facility license, licenses are required for all persons who operate or, in the words of the regulations, "... manipulate the controls of..." a reactor. Each potential operator is required to submit an application containing general information, education and training pertinent to reactor operations, previous licenses, and a medical examination report.

After the application is evaluated, the prospective operator is given written and oral examinations and an operating test to demonstrate ability to safely operate a reactor. Upon passing these tests, an operating license for a specific facility is issued (general operating licenses are not issued). Licenses are issued for a two-year period and can be renewed if certain conditions are met: demonstration of physical fitness and completion of an NRC approved requalification program or successful re-examination.

Two categories of licenses are issued: operator and senior operator. Both categories have written examinations covering fundamentals of reactor theory, design feature operating characteristics (both general and specific to the reactor for which the examination is being taken), radiological safety principles and procedures, and standard and emergency operating procedures of the facility.

The senior operator examination includes a more intensive examination of reactor theory, radiological safety and design, conditions and limitations (in the facility's operating license and technical specifications), reactivity changes, radioactive waste disposal and control of effluents, coolant chemistry and fuel handling.

With the operating tests, the examiners observe an applicant's ability to safely operate the reactor and to follow established procedures. The applicant must also demonstrate knowledge of all reactivity systems, and actions to be taken in the event of an emergency. Other test areas include:

Recognition of annunciator signals.
Radiation levels and hazards.
Unusual operating conditions.
Expected transients.

Reactor operation can be carried out by any licensed operator, but, because of necessary additional safety and back-up capability knowledge, a senior operator usually must be present in the control room. (In the case of small, nonpower reactors, one must be nearby in the facility.)

In some research/testing reactors, certain procedures are limited to senior operators. The senior operator carries the burden of responsibility for safety; and, at any reactor, the operations supervisor/director plus other key personnel are required to hold senior reactor operator licenses.

EXERCISES

1. Trace a flow pattern for licensing of a power reactor; include approximate time required for each step.
2. Identify role of states with regard to licensure and control of reactors.
3. Describe three principal areas of a PSAR.
4. What licensing requirements could a local building department impose on a large power reactor?

MATERIALS

None.

PROCEDURES

None.

DATA TABLE

None.

REFERENCE MATERIALS

Kathren, Ronald L. "Environmental Impact Statements of Nuclear Power Plants." Journal of Environmental Sciences 16 (September-October 1973)5:11.

LaMarsh, John R. Introduction to Nuclear Engineering. Reading, MA: Addison-Wesley Publishing Co., 1975.

U.S. Atomic Energy Commission. "The Safety of Nuclear Power Reactors and Related Facilities." WASH Report, No. 1250, July 1973.

________. Title 10, Code of Federal Regulations, Parts 1, 2, 9, 19, 20, 50, 51, 55, 70, 71, 73, 100, 115 and 140.

U.S. Nuclear Regulatory Commission. "Preparation of Environmental Reports for Nuclear Power Plants." Regulatory Guide, No. 4.2, 1976.

________. "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants." Regulatory Guide, No. 1.70 NUREG - 75/094, Rev. 2, September 1975.

AEC and NRC documents are available by writing the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

TEST

1. Explain legal bases of the reactor licensing process:

2. Indicate purpose and general content (of any four chapters) of a Preliminary Safety Analysis Report:

3. Indicate purpose and general content of an Environmental Report:

4. Briefly explain why it is important for nuclear facility personnel to be familiar with the Final Safety Report of the facility:

5. Indicate importance of facility and component design to safety (as described in this module):

6. This module describes a Preliminary Safety Analysis Report, Environmental Report and other licensing documents, including technical specifications. Briefly explain relationships between these documents:

7. Define:

   License.

Law.

Rule.

Regulation.

Regulatory Guide.

Environmental technical specifications (ETS).

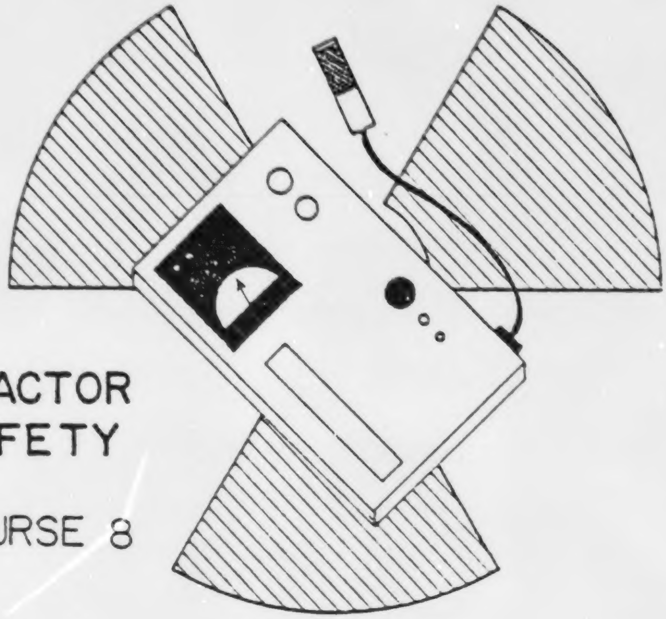
Safety technical specifications (STS).

8. Use a diagram; trace a Final Safety Report and an Environmental Report from their origins to their final application(s):

NUCLEAR TECHNOLOGY

MODULE 8-3 REACTOR PROTECTION SYSTEMS. -

RONALD L. KATHREN
PORTLAND GENERAL ELECTRIC COMPANY



REACTOR SAFETY

COURSE 8

81

TERC-SW

TECHNICAL EDUCATION RESEARCH CENTER — SOUTHWEST
4201 LAKE SHORE DRIVE WACO, TEXAS

COURSE MODULES

COURSE 8 REACTOR SAFETY

	MODULE 8-1	Introduction to Reactor Safety
	MODULE 8-2	Reactor Licensing
⇨	MODULE 8-3	Reactor Protection Systems
	MODULE 8-4	Reactor Emergency Systems
	MODULE 8-5	Safeguards and Security

Copyright in 1977 by the Technical Education Research Center, Inc. Printed in the United States of America. All rights reserved. These materials, or parts thereof, may not be reproduced in any form without permission.

The materials contained herein were developed pursuant to a contract with the Office of Education, U.S. Department of Health, Education and Welfare: Contract No. 300760356. Contractors undertaking such projects under Government sponsorship are encouraged to express freely their professional judgment in the conduct of the project. Points of view or opinions stated do not, therefore, necessarily represent official Office of Education position or policy.

Technical Education Research Center
Southwest
4201 Lake Shore Drive, Suite 111
Waco, Texas 76710

INTRODUCTION

A nuclear reactor - especially a nuclear power reactor - is a highly complex assemblage of systems with both manual and automatic controls to keep operating characteristics within required performance limits. Despite inclusion of redundant and multiple controls, and despite highly trained and competent operators, it is conceivable (though very unlikely) that a situation could occur in which the control function breaks down.

This module presents the general philosophy of reactor protection systems. Also, it provides an introduction to these systems and their operational characteristics and applications.

MODULE PREREQUISITES

The student should have completed Course 1, "Radiation Physics," Course 3, "Principles of Process Instrumentation," Course 5, "Introduction to Nuclear Systems," and Course 7, "Reactor Operations," or their equivalent. Also, the student should have completed the previous modules in this Course.

OBJECTIVES

Upon completion of this module, the student should be able to:

1. In one or two sentences, state basic philosophy and function of reactor protection systems.
2. Name at least four reactor protection systems.
3. Describe design requirements of protection systems.
4. List and describe, in two or three sentences, eight major design parameters for protection systems.
5. In one or two paragraphs, compare and contrast general and local coincidence logic and how these are applied.
6. Briefly state importance of testability as applied to protection systems.
7. In one sentence, differentiate between "safety margin" and "safety limit."
8. Set up a logic coincidence system for reactor shutdown, based on measurements of three variables in the core.

PHILOSOPHY AND DESIGN BASIS

The basic philosophy underlying reactor protection includes:

- To prevent reactor from exceeding safe operating limits.
- If limits are exceeded, to minimize or eliminate adverse consequences.

The reactor protection system is designed to protect plant employees and the public from radioactivity. In addition, it must prevent or minimize damage to the plant.

Protection includes a variety of systems:

- Reactor shutdown.
- Containment.
  - Emergency core cooling (ECCS).
  - Containment isolation.
  - Containment pressure reduction.
- Air cleaning
- Fire protection.
- Emergency power.

A reactor shutdown system is the total of all devices and electromechanical elements involved in emergency reduction of power level or reactivity. A shutdown system includes scram systems, safety rods and liquid poison (boric acid) injection systems.

The remainder of the protection system can be lumped into a broad category of engineered safety features. These safeguards include the ECCS, pressure reduction systems, auxiliary power supplies and similar systems not part of the emergency shutdown system.

Protection systems are designed by first analyzing potential accidents and their consequences, then specifying conditions that might lead to various postulated conditions and, finally, setting limits for safe reactor operation (Figure 8-3-1). Note continual assessment of impact (of

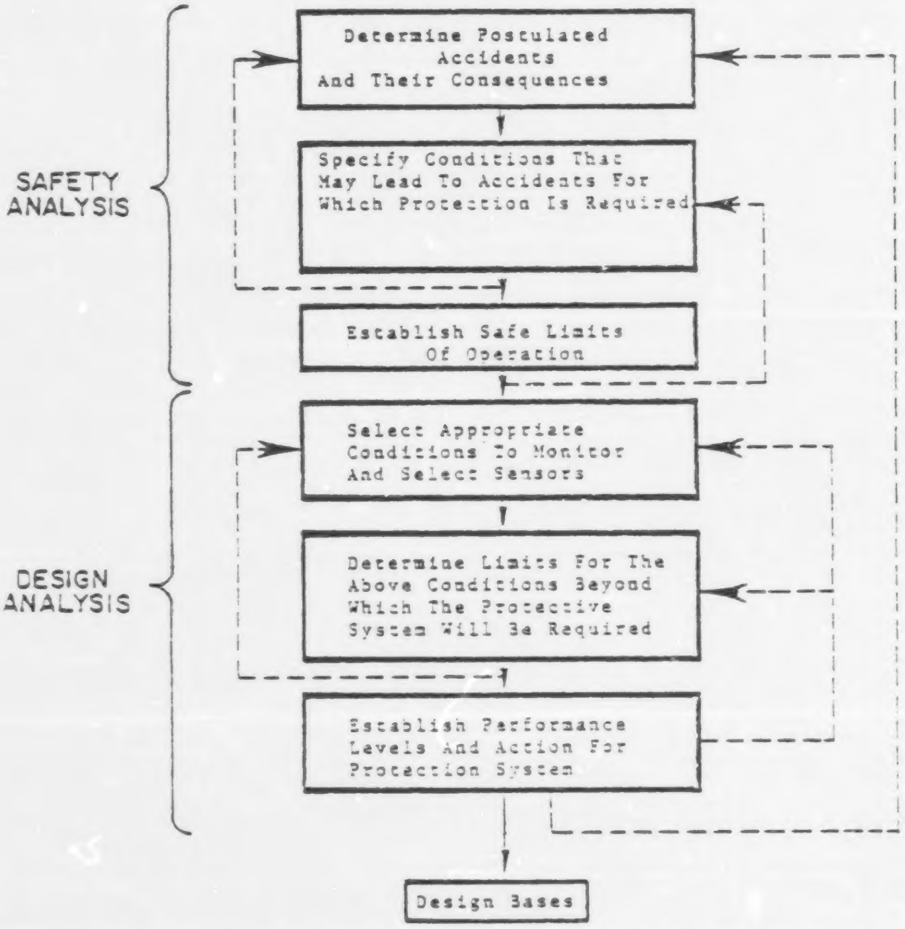

SAFETY ANALYSIS
Determine Postulated Accidents And Their Consequences
Specify Conditions That May Lead To Accidents For Which Protection Is Required
Establish Safe Limits Of Operation
DESIGN ANALYSIS
Select Appropriate Conditions To Monitor And Select Sensors
Determine Limits For The Above Conditions Beyond Which The Protective System Will Be Required
Establish Performance Levels And Action For Protection System
Design Bases

Figure 8-3-1. Sequence In Establishing Design Bases For Protection Systems. Note Feedback Loops Signifying The Interrelationships Between The Various Stages.

Figure 8-3-1. Sequence in establishing design bases for protection systems. Note feedback loops signifying relationships between various stages.

subsequent stages) on earlier considerations, as indicated by feedback loops (dashed lines). Note that the sequence is broken down into two basic parts, 1) safety analysis and 2) design analysis, which ultimately leads to establishment of a specific design basis for each protection system.

Once a safety analysis has been completed, various parameters to be monitored are selected and appropriate sensors are chosen. For example, a decision might be made to measure pressure differential between two specific sections of pipe (this parameter might be a direct indicator of a leak in the primary coolant system); measurement is only part of the design, however, because initiation of protective action (i.e., activation of the appropriate protection system) must occur when the measuring device indicates some predetermined level.

PROTECTION SYSTEM DESIGN

Safety analyses determine if safety protection systems are needed and, if so, their designs. Postulated accidents must be analyzed in detail to determine potential effects on public health and safety as well as the plant. Either a fault-tree diagram or an accident-sequence diagram (Figure 8-3-2) is used to show steps that could lead to an undesirable hazardous condition.

An important consideration in protection system design is the effects of a false signal activating the system. Spurious activation could have serious consequences and is, therefore, a logical and necessary part of the safety analy-

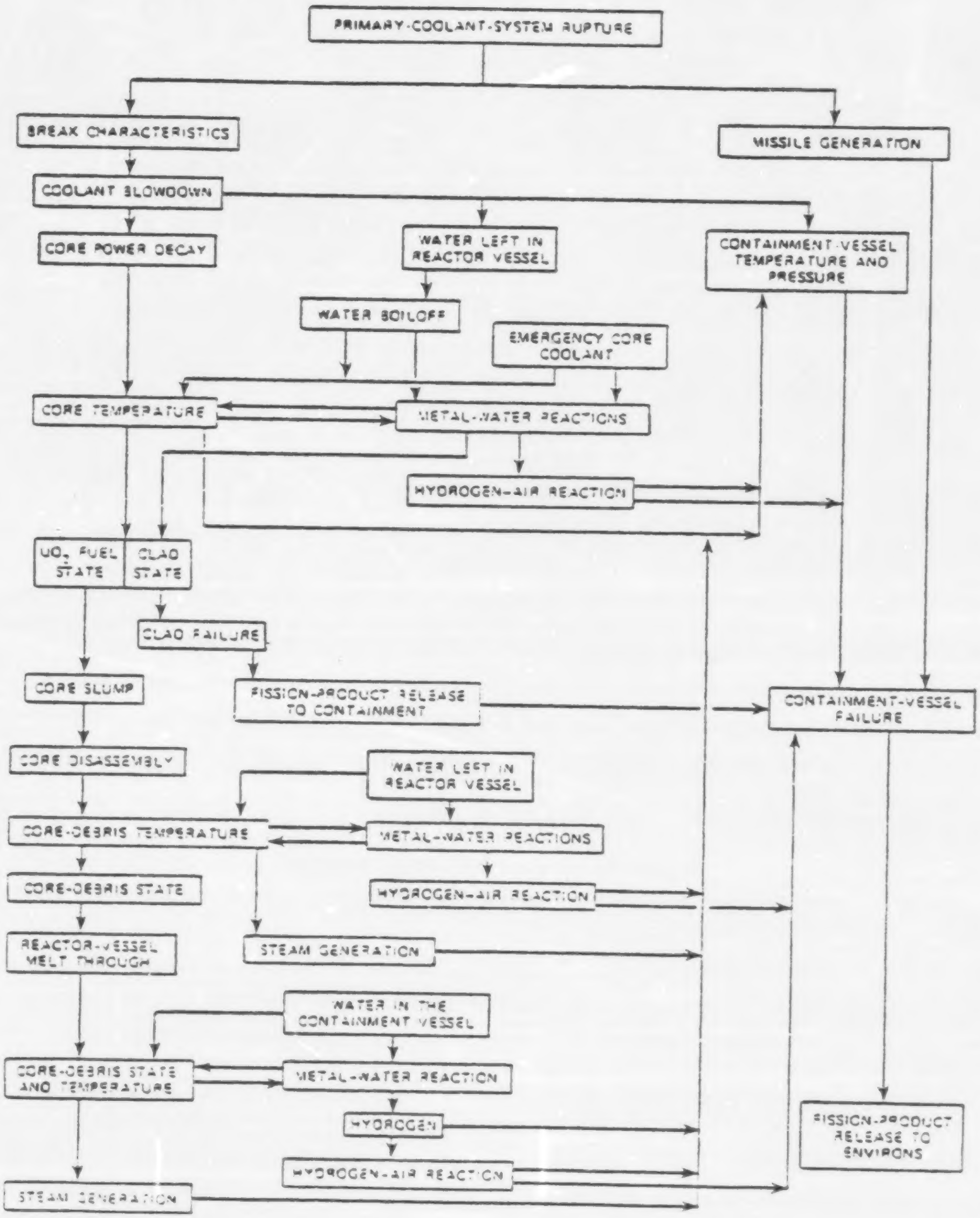

PRIMARY-COOLANT-SYSTEM RUPTURE
BREAK CHARACTERISTICS
MISSILE GENERATION
COOLANT BLOWDOWN
CORE POWER DECAY
WATER LEFT IN REACTOR VESSEL
CONTAINMENT-VESSEL TEMPERATURE AND PRESSURE
WATER BOILOFF
EMERGENCY CORE COOLANT
CORE TEMPERATURE
METAL-WATER REACTIONS
HYDROGEN-AIR REACTION
UO2 FUEL STATE
CLAD STATE
CLAD FAILURE
CORE SLUMP
FISSION-PRODUCT RELEASE TO CONTAINMENT
CONTAINMENT-VESSEL FAILURE
CORE DISASSEMBLY
WATER LEFT IN REACTOR VESSEL
CORE-DEBRIS TEMPERATURE
METAL-WATER REACTIONS
CORE-DEBRIS STATE
HYDROGEN-AIR REACTION
REACTOR-VESSEL MELT THROUGH
STEAM GENERATION
WATER IN THE CONTAINMENT VESSEL
CORE-DEBRIS STATE AND TEMPERATURE
METAL-WATER REACTION
HYDROGEN
HYDROGEN-AIR REACTION
STEAM GENERATION
FISSION-PRODUCT RELEASE TO ENVIRONS

Figure 8-3-2. Accident sequence for loss-of-coolant accident. (Adapted from McLain, USAEC Report ORNL-NSIC-23.)

sis. For example, a spurious low-pressure signal leading to actuation of the safety injection system might cause significant damage to a PWR. Or, BWR core damage might be incurred as a result of spurious automatic pressure relief. In addition, a spurious containment isolation could lead to shutdown of the reactor and, perhaps, activation of the emergency core cooling system.

STANDARDS AND REGULATIONS

Once the protection system has been designed, an analysis must be made of effects of its various protective actions. This analysis must consider whether functional protection requirements are met or, more specifically, whether the protection system meets legal requirements stipulated by law, regulations, standards and guides.

The regulations specify design criteria for protection systems. Appendix A to 10CFR50 is a listing of 64 General Design Criteria imposed on all nuclear power plants; Criteria 20 through 29 are specific to reactor protection systems. These include a statement of protection system functions followed by functional hardware-oriented guidelines. In addition, NRC may impose specific protection system requirements in the technical specifications (a part of every reactor operating license). Also, legal requirements for design are augmented by a series of Regulatory Guides published by NRC.

In addition to design criteria provided by NRC, various organizations have put forth design criteria for reactor protection systems. Such standards do not have the force of laws or regulations, but are sometimes included by reference in NRC Regulatory Guides. Criteria put forth in these standards might be considered good or acceptable practice and, wherever possible, engineering design should conform to recommendations of such standards.

The major standards-setting bodies with regard to reactor protection systems are the American National Standards Institute (ANSI), Institute of Electrical and Electronics Engineers (IEEE) and American Nuclear Society (ANS). ANS and IEEE are professional organizations whose standards are often adopted with little if any change by ANSI.

PLANT VARIABLES

Many plant variables affect design of protective devices and systems. Of paramount importance are plant safety limits - the specific value of a variable that cannot be exceeded without compromising safety. There are many safety limits, and often these cannot be directly ascertained. For example, many of the parameters associated with fuel elements, such as cladding temperature and hot spots, centerline temperatures, local flow rates, must be inferred or indirectly obtained from knowledge or measurement of other parameters such as cross section, heat transfer coefficients and flux levels.

An important plant variable (in a PWR) is departure from nucleate boiling ratio (DNBR), which is a function of power level, coolant temperature, pressure and flow, and other factors. (Where DNBR is too high, heat transfer from fuel to coolant is reduced, leading to possible melting of fuel.) If the limit, indicated by boundaries of an acceptable operating range (as determined by these power and coolant values) is exceeded, a reactor trip (i.e., a protection system) is activated.

DESIGN PARAMETERS

Certain basic features must be considered in design of protective devices and systems:

Safety margins.
Accuracy and range of instrumentation.
Response time.
Environmental factors.
Reliability.
Redundancy and diversity.
Independence.
Logic.

Safety margins, distinct from safety limits, are an important factor in design of a protection system. A safety margin is the difference between the level at which a protection feature is activated and the level at which damage will occur (safety limit). This difference, also known as trip margin, can be mathematically expressed:

Trip margin = level at which damage might occur
- level at which corrective system is actuated.

This margin also can be shown by consideration of power level (Figure 8-3-3).

When establishing safety or trip margins, transients, spikes (overshoots) and system accuracy need to be taken into account. Also, the margin between normal maximum operating points and trip points is important. A trip point should be set as close to maximum operating point as possible to provide maximum safety. But, this proximity may

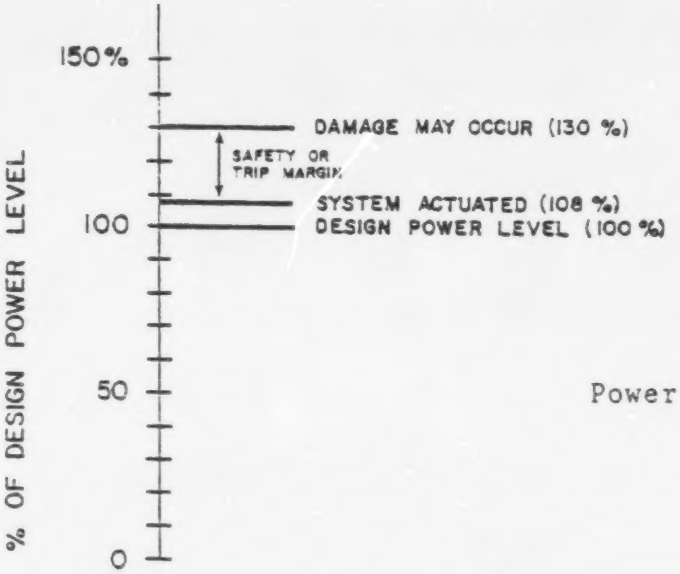

150%
100
50
0
% OF DESIGN POWER LEVEL
DAMAGE MAY OCCUR (130 %)
SAFETY OR TRIP MARGIN
SYSTEM ACTUATED (108 %)
DESIGN POWER LEVEL (100 %)

Figure 8-3-3.
Power level safety margin.

increase likelihood of a false trip. If, on the other hand, the trip point is set closer to the safety limit (safety margin is decreased), the probability of a false or spurious trip is reduced, but possibility of reaching the safety limit before the trip occurs is increased. The optimum point lies somewhere between the two and is always selected with the emphasis toward safety; that is, the trip point is set toward maximum operating level, increasing the safety margin.

Accuracy and range of instrumentation figure prominently in design. Generally, electronic measurements are highly precise. During an accident, however, a measured variable may take an extreme value with a relatively large measurement error. Other variables such as temperature, pressure and gamma radiation levels may also affect accuracy and produce larger measurement errors than during normal operation.

It is, therefore, important to set the trip level at a value that compensates for these possible influences. If the possible error is, say, ± 2%, trip level should be changed by 2% to compensate.

Instrument range must be selected such that an overrange or off-scale signal produces the desired response. In other words, no matter how far the signal falls outside the range of the instrumentation, it must produce an unsafe response or failure in the unsafe direction. To illustrate, many instruments read downscale (foldover) or saturate above a certain level. Thus, although trip point level is exceeded, the instrument may not say so (Figure 8-3-4), and this could lead to an unsafe condition. Overload foldover saturation (jamming or paralysis), a characteristic of most count rate systems, renders them unsatisfactory for protection systems unless specially designed. Overrange margins must always be adequate to accomodate extreme and unusual

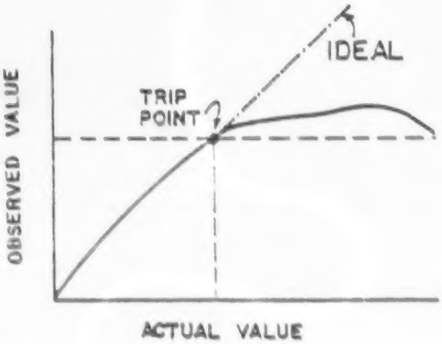


Figure 8-3-4.
Instrument saturation. As level rises, trip occurs, but may later reverse because of foldover.

levels. In addition, the system must not be rendered unusable by operating at normal levels for long periods.

Response time is the time delay from the time the trip signal is received until the emergency system reacts. It should be kept as short as possible, and must preclude delays from electrical and mechanical systems. Figure 8-3-5 illustrates effect of a 0.04-second time delay on a reactor overpower scram.

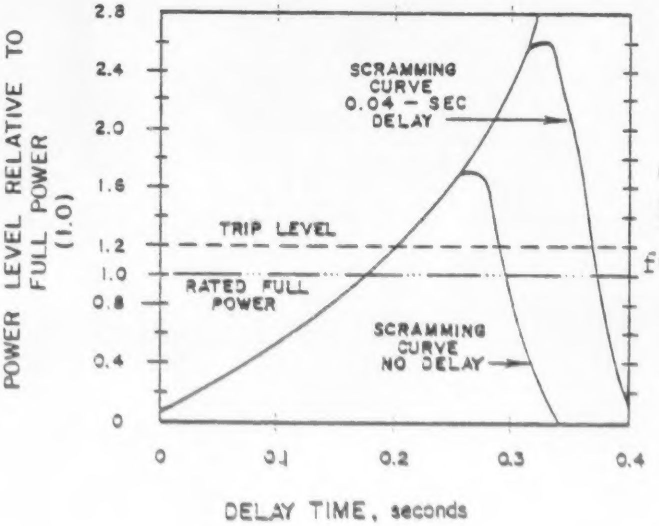


Figure 8-3-5. Overpower scram [reactor period is 0.1 second and trip level 120% (1.2) of full power] showing effect of a 0.04-second time delay. (Adapted from Schultz.)

In general, response time of an electronic system is a function of its time constant, or resistance-capacitance products; usually it can be kept small. Response time of mechanical systems (such as meters or control rods), which must move masses, generally is greater and the limiting factor.

The most time-dependent of all protection systems are those dealing with shutdown. These systems should be capable of very rapid response, since reactivity changes can occur quickly.

The classic startup accident (in which all control rods are similtaneously removed) provides an example of a reactivity change that can occur in a period so short that the speed of the accident could easily be great enough to render the shutdown system ineffective. In this case, another protection system - one to limit the number of rods that can be withdrawn at a time - is necessary. Note that such a system, which might feature interlocks on rod banks, is not time dependent.

Environmental factors, under accident conditions, may determine many design features. The protection system must not be rendered ineffective by the type of accident it is supposed to prevent or minimize. Extremes of temperature, pressure, neutron or gamma radiation, noise or vibration may occur. Portions of the protection system may be subjected to immersion, or normally immersed components suddenly may be thrust into dry air. Also, fire may result.

It is neither possible nor realistic to attempt to incorporate in a protection system a design to withstand all conceivable environments. The 64 General Design Criteria (listed in 10CFR50, Appendix A) require that protection systems withstand forces from natural phenomena greater than those known to have occurred in the vicinity of the site.

Reliability of a protection system is a function of both the probability that the protection system will be needed and consequences of failure of the system. General Design Criterion 21 specifically addresses reliability and testability of a protection system, noting that each system "... be designed for high functional reliability and inservice testability commensurate with the safety of the functions to be performed."

There are four modes of protection-system plant interaction:

Safe (normal).
Safe failure.
Unsafe failure.
Protected failure.

In mode 1 (safe), plant and protection system are operating within normal limits. In other words, the plant is operating within its design (or safe) limits and the protection system is not operating because it is not needed. This is, of course, the desired situation.

In mode 2 (safe failure), the plant is operating normally and within safe limits, but the protection system has been actuated unnecessarily. In mode 3 (unsafe failure), the reactor is outside safe limits and the protection system has failed to operate. In mode 2 and mode 3, reliability is unsatisfactory.

In mode 4 (protected failure), the reactor is operating outside safe limits, but the protection system has operated as designed; thus, the reactor is protected. Note that only in mode 3 (Figure 8-3-6) is there an unsafe situation, namely an unprotected accident.

Reactor Condition	Protection Off	System Activated
Normal	Mode 1: Safe	Mode 2: Safe Failure
Outside Safe Limits	Mode 3: Unsafe	Mode 4: Protected

Figure 8-3-6. Possible relationships between reactor condition and protection system condition.

Probability (or rate) of an unprotected accident or unsafe condition can be calculated easily as the product of the probability of unsafe operation and the probability of protection system failure. The latter is merely a measure of reliability. Ordinarily, safety analyses consider probability of failure of the protection system to be in the neighborhood of 10^{-6} per reactor year. In other words, probability for such an accident in a given reactor in a year's time is one chance in a million. Probability of unsafe operation that could lead to an accident may be as great as 1 per reactor year. If so, probability of protection system failure cannot exceed 10^{-6} per reactor year to maintain the allowable acceptable risk for an unprotected accident at 10^{-6} per reactor year. Thus, reliability of the protection system must be $1.0 - 10^{-6} = 1.0 - 0.00001 = 0.99999$ or 99.9999%.

Implicit in the concept of reliability is testability, or the means to determine and verify operational status of the protection system. The design must properly include provision for periodic testing of system function while the reactor is in operation. It must also provide a means for evaluation of performance failures. (Performance failures are those in which the protection system partially functions but is not able to completely perform the desired task. Such failures are usually the result of improper or inadequate design or unsatisfactory design bases.)

Redundancy and diversity (multiplicity) are methods of increasing reliability. The single failure criterion, which is the basis for redundancy, may be simply stated: "No single failure shall result in system failure." Thus, failure of one element or component or one of two or more redundant or diverse systems should still leave the reactor with an operational protection system.

Independence of redundant systems, which is of sufficient importance to be specifically called out by a General Design Criterion, refers to freedom of any one system, channel or component from operational dependence on another. If the failure of a single component (for example, a motor-operated valve) would render two redundant safety systems inoperative, the systems are not independent. Again, a common mode failure has been described. Physical separation of components, elements and systems, electrical isolation and separate protection for key system elements are some of the ways used to achieve such protection. The goal, of course, is to prevent a single event from rendering the entire protection system useless.

Logic, the final design element, refers to the sequence and handling of signals to produce the desired protection response. As with any aspect of a protection system, serviceability of the system, while important, is secondary to safety. Hence, where a clear choice is offered between safety and serviceability, the former must always prevail.

For safety, it is preferable and, in most cases, mandatory that protection system logic elements be fail-safe; that is, an element failure, spurious signal or loss-of-power must induce the protective response. Fail-safe design could be extended to include induction of protective action if any type of anomaly is noted in the system. For example, a temperature rate-of-change detector might cause a false trip and initiate the containment spray system. In other words, it would function in exactly the opposite manner as well as in the manner it should.

Obviously, there are limits to fail-safe, for improper extension could produce an unacceptable number of mode 2 (safe failure) conditions while not increasing safety. Fail-safe design, like system independence, can never be complete. Thus, provision should be made to employ testing to detect failures and to verify system operation.

Perhaps the single most useful concept in fail-safe design logic is the use of signal loss (or de-energizing) to activate a desired protective feature (Figure 8-3-7). The safety rod is held above the core by an electromagnet that, when energized, grips a steel plate welded to the rod; power failure de-energizes the magnet, allowing the rod to fall into the core and shut down the reactor.

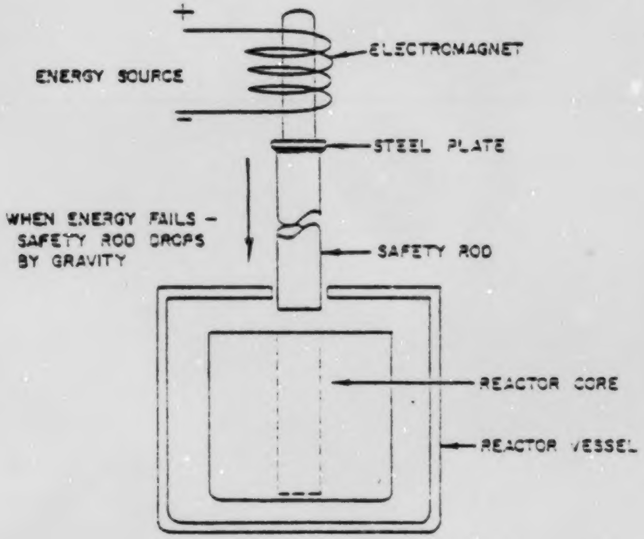

+
ELECTROMAGNET
ENERGY SOURCE
−
STEEL PLATE
WHEN ENERGY FAILS – SAFETY ROD DROPS BY GRAVITY
SAFETY ROD
REACTOR CORE
REACTOR VESSEL

Figure 8-3-7. Simple fail-safe shutdown system.

To improve protection system serviceability, coincidence logic is used. By requiring two or more simultaneous signals to initiate an action, the safe-failure mode can be minimized. In addition, a single channel can be tested under operating conditions without bypassing or actuating the system. There is a small penalty with respect to safety, for a coincidence system requires at least two functional signals and there is a small but real chance that, in an accident situation, only one signal may be generated. This probability can be reduced to more than acceptable levels by use of the "2 out of n" technique, which uses n detectors or signals, any two of which initiate the protective action.

Coincidence logic can be divided into two broad categories: local and general. In local coincidence logic (Figure 8-3-8), output signals for a single plant variable are fed into the logic circuit. Any two of these signals are adequate to actuate the protection system. (Local coincidence is also called individual, specific or single-parameter coincidence.)

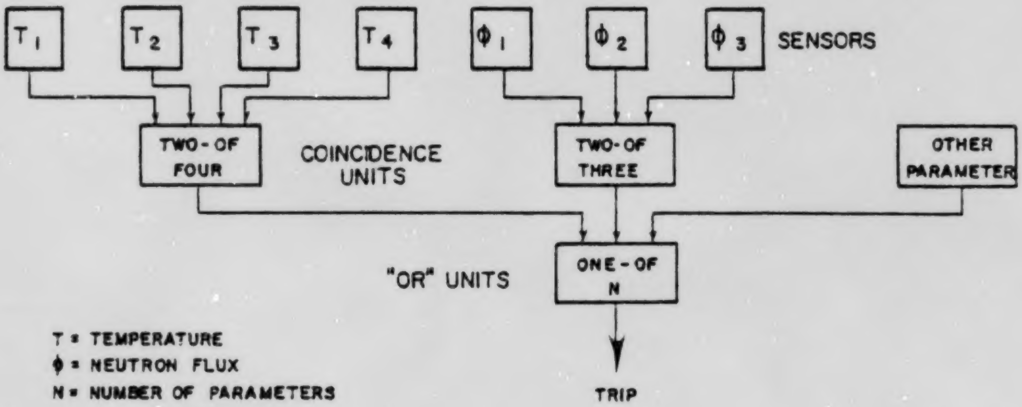

T1
T2
T3
T4
Φ1
Φ2
Φ3
SENSORS
TWO-OF FOUR
COINCIDENCE UNITS
TWO-OF THREE
OTHER PARAMETER
"OR" UNITS
ONE-OF N
T = TEMPERATURE
Φ = NEUTRON FLUX
N = NUMBER OF PARAMETERS
TRIP

Figure 8-3-8. Local coincidence logic.

In general coincidence logic, output signals for several plant variables are fed into the logic circuit (Figure 8-3-9). Any two signals or any two signals of the same parameter cause actuation of the protection system. General systems are also known as multi-parameter, mixed, or guardline coincidence and, although somewhat less reliable from a mode 2 standpoint, are clearly superior from a safety standpoint.

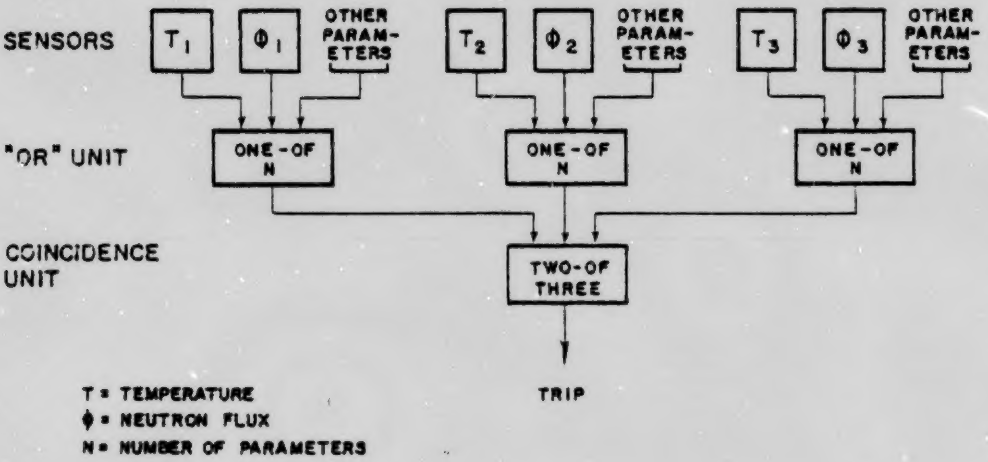

SENSORS
T_1
Φ_1
OTHER PARAMETERS
T_2
Φ_2
OTHER PARAMETERS
T_3
Φ_3
OTHER PARAMETERS
"OR" UNIT
ONE-OF N
ONE-OF N
ONE-OF N
COINCIDENCE UNIT
TWO-OF THREE
TRIP
T = TEMPERATURE
Φ = NEUTRON FLUX
N = NUMBER OF PARAMETERS

Figure 8-3-9. General coincidence logic.

TESTING AND MAINTENANCE OF PROTECTION SYSTEM

Protection system design is only one part of the protection problem.

Once installed, periodic testing is necessary to ensure that the system is operational. In power reactors, which are designed for continuous operation, capability for in-service testing must be provided so that the reactor need not be shut down.

Whenever possible, protection systems should be designed to permit maintenance and even repair while the reactor is in operation. This is of particular importance for power reactors because of economic considerations of shutdown. Of course, safety must not be compromised during such activity, and replacement of components must be strictly limited to identical times.

Other operational considerations of protective systems include provision for completion of the protective action once it has been started. Thus, a shutdown system should completely shut the reactor off - not just reduce power level. Manual trip provisions, in addition to automatic features, should be included in the design, as should protective interlocks to block certain sequences of events that might destroy capability of the system to respond.

A final operational consideration is protection system status as a whole, as well as that of each subsystem. This status, which should be clearly and concisely displayed or otherwise available to the operator, includes:

An indication of overall condition.

A readout or indication of each variable used to initiate a protection signal.

An indication of bypasses and channels removed from service.

Position or condition of actuators.

Operating mode status.

Test status.

Accumulated life.

Also, the operator is required to acknowledge any indication of system failure or malfunction prior to taking any positive action to reset or defeat the system.

EXERCISES

1. Discuss trade-offs between safety and serviceability; show how coincidence logic affects each.
2. Sketch (a block diagram) a logic coincidence system for a reactor shutdown; use the following parameters:
   - Overpower measurement.
   - Coolant temperature.
   - Neutron flux.
3. A rod drive motor has a safety limit of 806°F: this temperature is reached at 107.8% of full rated power. The overpower scram system, which relies in part on that motor, is set to trip at 106.5%. What is the safety margin? What is the margin if sensor accuracy is ± 2% of its full-scale reading (which is 120% of full rated power)?

MATERIALS

None.

PROCEDURES

Write a library or research report concerning a nuclear power reactor incident. Specifically, the following should be listed:

Description of incident and its probable causes.
Reactor or protective components affected by incident.
Design feature(s) that failed, and why.
Design feature(s) that performed effectively to limit effects of incident.

DATA TABLE

None.

REFERENCE MATERIALS

American National Standards Institute. "Criteria for Preparation of Design Bases for Systems That Perform Protective Functions in Nuclear Power Generating Stations." ANSI Draft Standard N18.8, 1973.

Available by writing the American Society of Mechanical Engineers, United Engineering Center, 345 East 47th St., New York, NY 10017.

Green, A.E. and Bourne, A.J. Reliability Technology. New York: John Wiley and Sons, 1972.

Hannauer, S.H. and Walker, C.S. "Design Principle of Reactor Protection Instrumentation Systems." USAEC Report ORNL-NSIC-51, September, 1968.

Available by writing the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

Institute of Electrical and Electronics Engineers. "Criteria for Protection Systems for Nuclear Power Generating Stations." IEEE Standard 279, 1971.

Available by writing Institute of Electrical and Electronics Engineers, 345 E. 47th Street, New York, NY 10017.

McLain, H.A. "Potential Metal-Water Reactors in Light Water-Cooled Power Reactors." USAEC Report ORNL-NSIC-23, August, 1968.

O'Brien, H.G. and Walker, C.S. "Protection Instrumentation System in Light Water-Cooled Power Reactor Plants." USAEC Report ORNL-NSIC-29, October, 1969.

The two above USAEC documents available by writing the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

Thompson, T.J. and Beckerley, J.G., eds. *The Technology of Nuclear Reactor Safety*. Cambridge: MIT Press, 1964.

United States Atomic Energy Commission. Title 10, *Code of Federal Regulations*, Parts 50 and 100.

See especially Appendix A to Part 50.

Available by writing the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

TEST

1. State (in terms given in this module) the basic philosophy and function of reactor protection systems:

2. List four examples of reactor protective systems (discussed in this module):
   (1)

   (2)

   (3)

   (4)

3. Describe design requirements of protection systems in general, with particular consideration for legal requirements as opposed to standards:

4. List eight important design parameters used in protection systems; briefly describe each:
   (1)

(2)

(3)

(4)

(5)

(6)

(7)

(8)

5. Illustrate by means of a block diagram general and local coincidence; describe how each is applied:

108

6. Briefly describe importance of testability, as applied to protection systems:

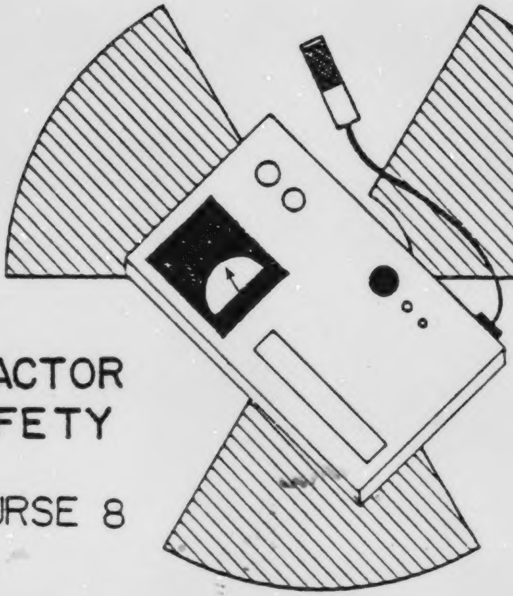
7. Briefly define difference(s) between safety margin and safety limit:

8. Briefly describe (use sketches as needed) a logic coincidence system for reactor shutdown (based on measurements of three core variables provided by instructor):

NUCLEAR TECHNOLOGY

MODULE 8-4 REACTOR EMERGENCY SYSTEMS. -

RONALD L. KATHREN
PORTLAND GENERAL ELECTRIC COMPANY



REACTOR
SAFETY

COURSE 8

TERC-SW

TECHNICAL EDUCATION RESEARCH CENTER — SOUTHWEST
4201 LAKE SHORE DRIVE WACO, TEXAS

COURSE MODULES

COURSE 8 REACTOR SAFETY

MODULE 8-1	Introduction to Reactor Safety
MODULE 8-2	Reactor Licensing
MODULE 8-3	Reactor Protection Systems
MODULE 8-4	Reactor Emergency Systems
MODULE 8-5	Safeguards and Security

Copyright in 1977 by the Technical Education Research Center, Inc. Printed in the United States of America. All rights reserved. These materials, or parts thereof, may not be reproduced in any form without permission.

The materials contained herein were developed pursuant to a contract with the Office of Education, U.S. Department of Health, Education and Welfare: Contract No. 300760356. Contractors undertaking such projects under Government sponsorship are encouraged to express freely their professional judgment in the conduct of the project. Points of view or opinions stated do not, therefore, necessarily represent official Office of Education position or policy.

Technical Education Research Center
Southwest
4201 Lake Shore Drive, Suite 111
Waco, Texas 76710

INTRODUCTION

This module focuses on emergency systems in reactors. It deals, exclusively, with ways to prevent or minimize accidents.

MODULE PREREQUISITES

The student should have completed Course 1, "Radiation Physics," Course 3, "Principles of Process Instrumentation," and Course 5, "Introduction to Nuclear Systems." In addition, the student should have completed all the preceding modules in this Course.

OBJECTIVES

Upon completion of this module, the student should be able to:

1. Describe general relationships of various reactor emergency systems and give two basic purposes for them.
2. Describe functions, general logic and types of emergency reactor shutdown systems.
3. List ten parameters used to actuate an emergency shutdown and explain why each is important.

4. Draw a schematic diagram of an emergency core cooling system in a PWR and in a BWR.
5. Explain differences between BWR and PWR emergency core cooling systems.
6. Describe emergency cooling system for a gas-cooled reactor; explain how it differs from an emergency core cooling system for a water-cooled reactor.
7. Explain applications of emergency radiation monitoring systems; describe specific applications in reactors.
8. Define:
    - Cold water accident.
    - ECCS.
    - CACS.
    - General design criterion.
    - ARMS.
    - PRMS.
    - Fire detection.
    - Fire prevention.
    - Fire suppression.

PURPOSE OF REACTOR EMERGENCY SYSTEMS

An emergency system is any system or apparatus designed to function rapidly (when needed) to prevent or minimize consequences of an accident. Thus, any system that offsets effects of operator error, equipment malfunction or reactor operation outside prescribed limits is an emergency system. These include non-nuclear systems, such as fire protection systems, security warning systems and even radio communication networks. Reactor emergency systems, of course, are those that pertain specifically to the reactor, and include protection systems as well as non-nuclear emergency systems and radiation monitoring systems (Figure 8-4-1). This illustration, which is by no means complete, merely indicates the diversity and breadth of a typical emergency system.

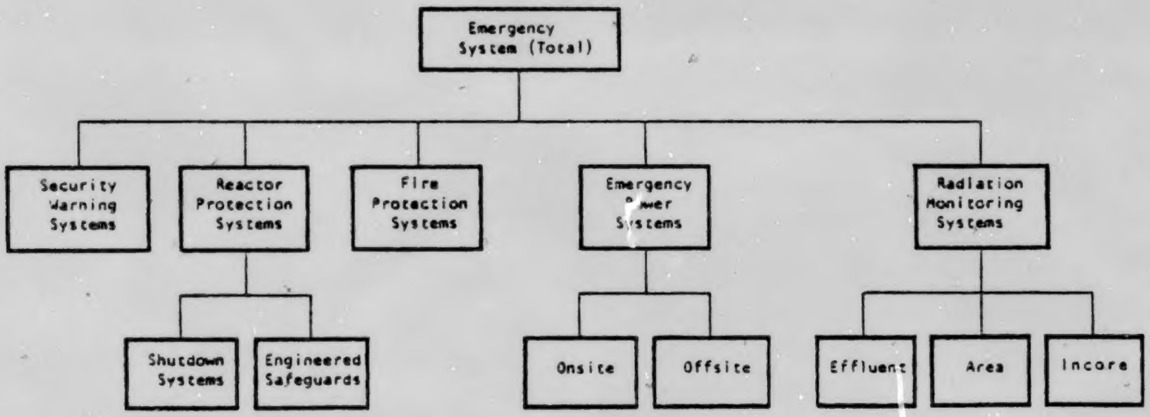

Emergency System (Total)
Security Warning Systems
Reactor Protection Systems
Fire Protection Systems
Emergency Power Systems
Radiation Monitoring Systems
Shutdown Systems
Engineered Safeguards
Onsite
Offsite
Effluent
Area
Incore

Figure 8-4-1: Relationships of various reactor emergency systems.

In reactor operations, the term emergency system is sometimes used as if it were synonymous with engineered safeguards, which gives it a protective function that is limited (in a radiological sense). This connotation is not strictly correct, nor does it adequately serve to describe the complete function. In this Course, the term emergency system includes at least those important non-nuclear systems that have emergency functions.

The basic purpose of any emergency system is to prevent, limit or control a situation before it leads to an accident. Obviously, this cannot always be accomplished; thus, a secondary aspect of an emergency system is to minimize effects of the accident.

REACTOR SHUTDOWN SYSTEMS

A reactor shutdown system, a part of the reactor protection system, is designed to prevent hazardous releases of radioactivity and, secondarily, to protect the core from damage.

Shutdown is not like the familiar go/no-go action of turning off a light, which, by interrupting the flow of electricity, completely extinguishes the action. Rather, reactor shutdown is accomplished by insertion of neutron-absorbing rods or liquids to reduce fission power output to insignificant levels; however, the reactor core still will have a significant thermal power level as well as a large inventory of radioactive fission products.

Emergency shutdown is known as "scramming" (or tripping off) the reactor; thus, a scram is a rapid shutdown, usually by deliberate, rapid insertion of control rods and safety rods. Scramming can be accomplished manually or automatically. A manual scram is induced by an operator for whatever reason is considered advisable. An automatic scram is the function of a system specifically designed to initiate the scram upon detection of an abnormal condition. Parameters most often used to initiate an automatic scram include:

Power level (overpower scram).
Period (short period scram).
Core temperature (excessive).
Coolant temperature (excessive).
Coolant flow rate (low flow).
Coolant pressure (too high or too low).
Coolant level (too low)
Radioactivity levels (primary, secondary or area).
Major reactor support system failure (electrical).
Significant shutdown in balance of plant.

For each reactor, an allowable range of power, pressure, temperature and neutron and radiation levels is defined, and these characteristics are continually monitored by sensors. If a characteristic exceeds its range, a trip is initiated by an automatic safety feature. Both overpower and period scram systems function to protect against reactivity excursions, which may result from uncontrolled or too rapid control-rod withdrawal, or from a so-called cold water accident.

A cold water accident is more likely to occur in a PWR because they have strong negative coolant temperature coefficients at operating temperatures. Injection of cold water (as from an inoperative loop) during normal operation causes a rapid rise in reactivity, which gradually comes down as coolant temperature rises. The sudden increase in reactivity produces a temporary increase in power level (as well as multiplication), and the power level increase could be sufficient to exceed reactor power safety limits.

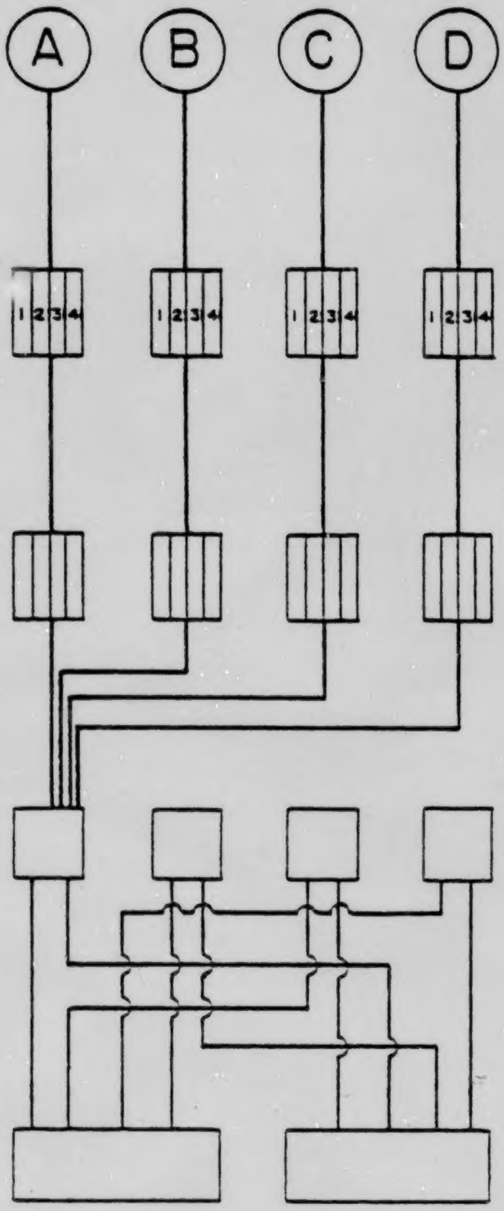
In a BWR, a sudden input of cold water also produces a reactivity change, primarily through lowering the void coefficient and, to a lesser extent, because of changes in temperature coefficient. In general, a BWR is less susceptible to cold water induced reactivity change. (Gas-cooled and liquid metal reactors are not susceptible at all.)

PWR overpower scram systems are generally actuated at ~ 112% or less of full rated power (Figure 8-4-2). The overpower and over-temperature ΔT trip points shown for a typical (but hypothetical) PWR operating at 2000 psia give an indication of the effect of uncertainty in instrument reading (accuracy) on trip point setting.

Overpower protection is usually provided by four power range, neutron flux channels with 2 out of n logic; i.e., trip requires two of the four detectors to be out of range (high). Each channel has an overlapping series of neutron detectors that provide signals not only for neutron flux, which is proportional to reactor output power level, but also for determination of the out-of-range period.

Note that the coincidence logic requirement (Table 8-4-1) is usually 2 out of 4. The list in this table, by no means exhaustive, merely indicates the types of scram systems commonly used in most BWR's and PWR's.

For scram or emergency shutdown, reactivity should be reduced at a rate that is from 10 to 100 times faster than the insertion rate for power control. Higher rates are of



Instrumentation and logic system power supplies for each of 4 redundant systems

Instrument channels (4 for each parameter or variable monitored)

1 of n logic - any channel for any parameter causes trip to next step

2 of 4 logic - any two of above cause trip to next step (only A system shown)

1 of 2 logic - trip in either system causes shutdown

Figure 8-4-2. Simplified logic diagram of a typical reactor shutdown system.

TABLE 8-4-1

SUMMARY OF A BWR-PWR SCRAM (EMERGENCY SHUTDOWN)

SCRAM SYSTEM	LOGIC	PRIMARY PURPOSE/COMMENT
Manual	1 of 2	Any reason, operator initiated
High Neutron Flux (Source, Intermediate and Power Ranges)	2 of 4	Core damage protection; may also be period scram
Coolant Overtemperature	2 of 4	DNBR protection in PWR, core protection in BWR
Core Overtemperature	2 of 4	Core protection
Overpower	2 of 4	May be based on ΔT in PWR; core protection
Low Pressurizer Pressure	2 of 4	Protects against core steam voids (DNBR protection) in PWR
High Pressurizer Pressure	2 of 4	Limits range required for over-temperature scram system (PWR)
High Pressurizer Water Level	2 of 3	Backup to high pressurizer scram (PWR)
Reactor Vessel High Pressure	2 of 4	Protects nuclear system process carrier
Coolant Low Flow (PWR) or Level (BWR)	2 of 3	DNBR protection (PWR) and core protection (PWR, BWR)
Undervoltage or Underfrequency	2 of 4	Protects against loss of scram or safety systems function
Safety Injection System	Depends on System Monitored	Scram follows actuation of safety system
Turbine	2 of 3	Heat dumping, core and overpower protection in BWR
Containment Pressure	2 of 4	Minimizes fuel damage in BWR; indicative of primary system break
Primary Radiation	2 of 4	Core protection; indicates fission break
Feedwater	2 of 3	Overtemperature protection
Low Steam Generator Water Level	2 of 4	Protects against excess pressure and overtemperature

little additional benefit because, after reactivity becomes a negative 1% ($\Delta K/K = 0.01$), reactor power decreases as the delayed neutrons decrease. Generally, there is a small time lag or release time between the time the scram signal is received and the time the scram action is initiated. This time must be kept as short as possible, since even a small delay in initiating shutdown can result in large power excursions. In practice, release times range between 10 and 50 msec. Scram time for a BWR or PWR generally ranges between 1 and 3 seconds.

As with light-water reactors, gas-cooled reactors also are equipped with emergency shutdown systems; however, because of inherent reactivity and coolant differences between gas-cooled and light-water reactors, there are significant differences in their respective shutdown systems. The CO_2-cooled British Magnox reactors use primarily a two out of three logic, having three protection channels into which all measured parameters are fed. Thus, system logic is a general coincidence, and primary shutdown parameters are excess flux at 1) low, intermediate and full power, 2) power doubling time (i.e., period), 3) coolant pressure, 4) rate of change and rate of flow, 5) coolant outlet temperature, and 6) fuel element temperature.

High-temperature gas-cooled reactors (HTGCR) with graphite cores and fuel elements can endure large power excesses and over-temperatures without damage. Thus, they have large safety limits, and can be built with large safety margins. Unlike a light-water reactor, an HTGCR uses graphite-clad fuel elements, which do not provide a definitive damage point (such as the melting temperature of zirconium or stainless steel claddings used in light-water and some research reactors).

Because graphite-clad fuel elements are susceptible to damage from steam or water, however, coolant gas moisture level is an important scram parameter. This condition usually is indicative of steam generator leakage. HTGCR's in the U.S. are equipped with coolant moisture detectors. Other common shutdown systems are based on 1) neutron flux in the power range, 2) flux change rate (period) and 3) reactor pressure.

A simplified scram system for a gas-cooled reactor includes two redundant logic systems. Similar logic arrangements are generally common to all reactor shutdown systems.

In addition to the common systems mentioned above, a newer GCR has several shutdown systems based on pressure measurements:

Reactor pressure.
Reheat steam pressure.
Superheat steam pressure.
Reheat steam temperature.
Plant electric power.
Reactor building temperature.

All of these are based on 2 out of 3 logic.

Only a single operational submarine reactor (since altered to a PWR) and power reactor have been built in the U.S. using sodium as a coolant; however, the liquid metal fast breeder reactor (LMFBR) demonstration plant, if it ever becomes operational, may presage the advent of many sodium-cooled units. As with other reactors, sodium-cooled units have scram parameters based on period and power level. Also, they have several types of sensors for scram actuation based on coolant flow and temperature. So important is the coolant flow that 1 out of 1 coincidence logic is used at EBR-2 (an experimental reactor) and at Dounreay (in Scotland).

EMERGENCY CORE COOLING SYSTEMS

No reactor emergency systems have received more attention from the general public and nuclear critics than the emergency core cooling system (ECCS). The ECCS was conceived as a means by which the core could be kept sufficiently cool following a major loss-of-coolant accident (LOCA) to prevent the fuel from melting and releasing radioactivity. Indeed, the ECCS was thought of as an inexpensive substitute for containment since, without meltdown, large releases of radioactivity could not occur.

To some nuclear scientists and reactor engineers, ECCS is considered part of the emergency shutdown system - it is designed to inject a borated or other poison-containing solution into the core.

ECCS is not a shutdown system, however; the neutron-absorbing poisons are included to offset moderating effects, and increased reactivity, caused by addition of water to a bare (or partially bare) core.

ECCS is necessary only at large power reactors or other reactors where fuel, if deprived of coolant, could get sufficiently hot (from decay heat plus residual heat in the fuel at time of shutdown) to melt down. Such would be the case following a major or dramatic coolant loss or a design basis LOCA.

Because of the inherent differences in design and cooling methods, ECCS and associated systems are quite different for PWR's, BWR's and HTGCR's.

In a PWR, ECCS consists of both an active and a passive system (Figure 8-4-3). The passive system, also known as

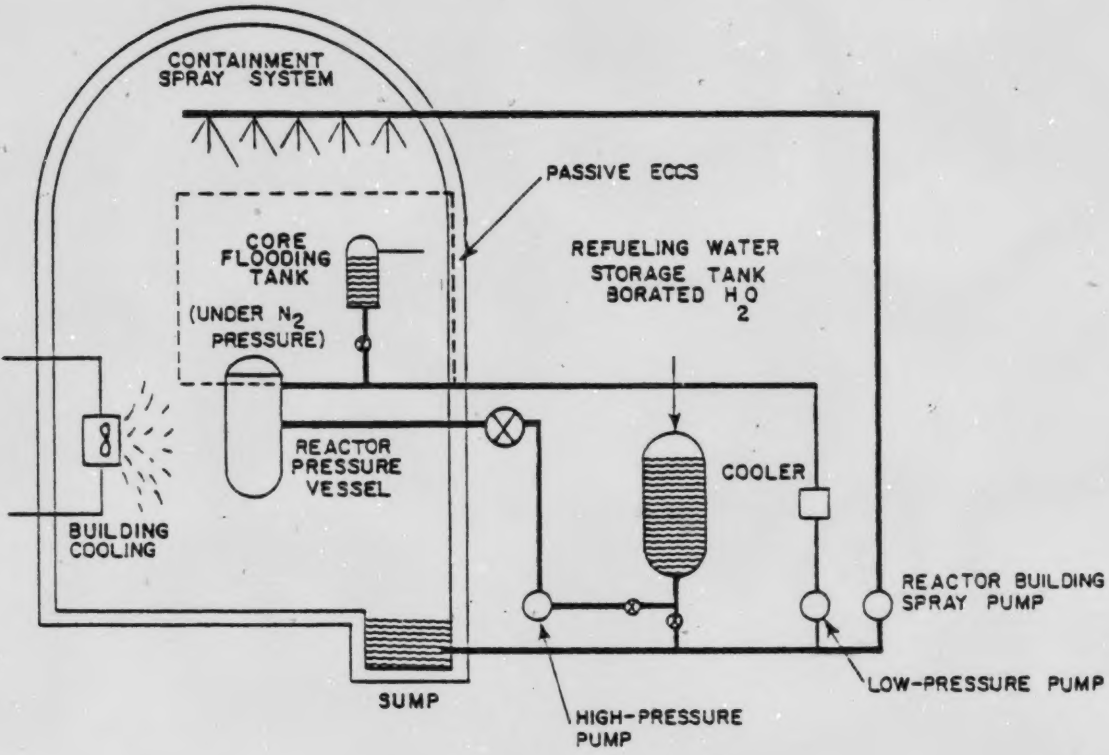

CONTAINMENT SPRAY SYSTEM
PASSIVE ECCS
CORE FLOODING TANK
(UNDER N_2 PRESSURE)
REFUELING WATER STORAGE TANK BORATED H_2O
REACTOR PRESSURE VESSEL
COOLER
BUILDING COOLING
REACTOR BUILDING SPRAY PUMP
LOW-PRESSURE PUMP
SUMP
HIGH-PRESSURE PUMP

Figure 8-4-3. Emergency core cooling system for a PWR.

the "accumulator injection system," is comprised of large accumulator tanks, generally one per primary loop, connected through check valves to piping between the main coolant pumps and the reactor vessel, or directly to the reactor vessel. These tanks contain borated water under a blanket of nitrogen at a pressure of 200 to 650 psi, usually toward the higher rate than the lower level. When pressure inside the reactor vessel drops below pressure of the cover gas in the accumulator tanks, the borated water solution is forced out through check valves into the reactor core through the cold legs of the primary coolant loop. (In the event of an

LOCA, a major pressure drop occurs in the reactor vessel.)

A passive ECCS (core flooding tank) requires no motors, pumps, motor-operated valves or other such equipment.

An active ECCS (in a PWR) has both a low- and a high-pressure coolant injection system. The low-pressure system pumps water from the refueling water-storage tank (or containment sump). It is designed to continue to inject emergency core cooling water for relatively long times after the passive accumulator tanks have been emptied. The low-pressure system also is used, following normal shutdown, to remove decay heat from the core (it is a recirculating system, passing coolant through heat exchangers).

The high-pressure system provides cooling water in the event of a small pipe break or other occurrence in which primary coolant pressure remains high. Charging pumps from the chemical shim system (boron injection system) pump water from the storage tank through the boron injection tank into the cold legs of the primary coolant system.

Typically, a BWR ECCS includes a high-pressure coolant injection system (early BWR) or spray system (later BWR). (It also may include independent low-pressure spray and injection systems.) The high-pressure system functions in the event of a small break or leak in the primary coolant system (one that does not produce rapid depressurization). If the water level in the reactor vessel drops below some predetermined height, this delivers its full flow within 25 seconds.

Additional water supplied by this system, first from the condensate water storage tank and then from the suppression pool, is delivered by a high-pressure, steam-powered, turbine-driven pump through a ring of nozzles over the core.

If the high-pressure system cannot maintain the water level, the reactor vessel is automatically depressurized by pressure-relief valves on the main steam line piping of the primary coolant system. These valves discharge high-pressure steam into the pressure suppression pool, through the reactor drywell (Figure 8-4-4). Automatic depressurization is

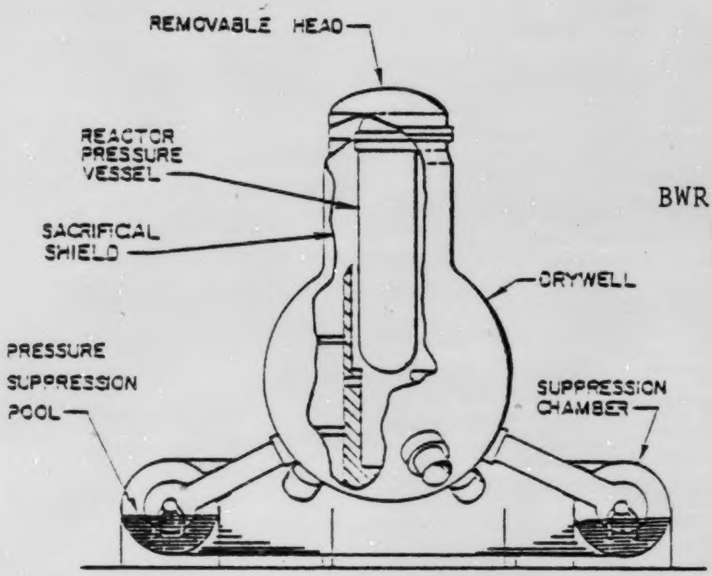

REMOVABLE HEAD
REACTOR PRESSURE VESSEL
SACRIFICAL SHIELD
DRYWELL
PRESSURE SUPPRESSION POOL
SUPPRESSION CHAMBER

Figure 8-4-4. BWR primary containment system. (Adopted from WASH-1250.)

not needed if a large break occurs in the primary system because the pressure drop is substantial.

In either case, depressurization actuates the low-pressure core spray (Figure 8-4-5) and coolant injection systems (Figure 8-4-6). The low-pressure core spray system has independent loops that spray water through a ring of nozzles onto the top of the core. The water is obtained from the pressure suppression pool and is pumped through a pair of redundant, electrically driven centrifugal pumps, each with sufficient capacity to provide adequate cooling to the core

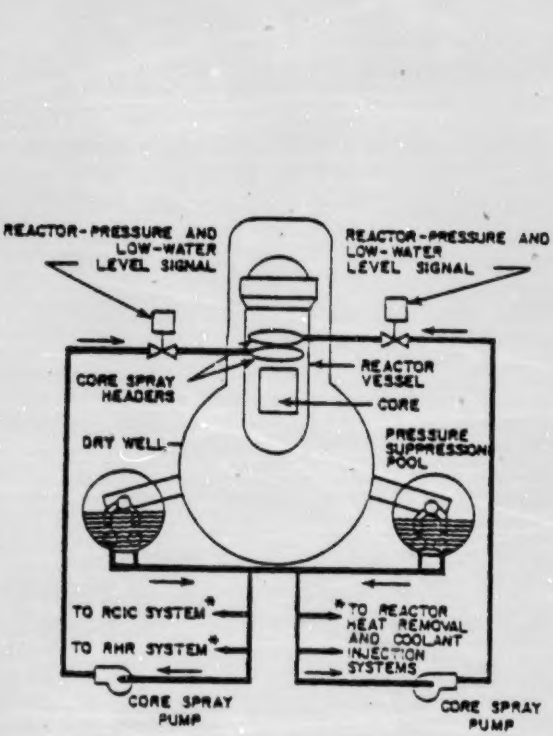
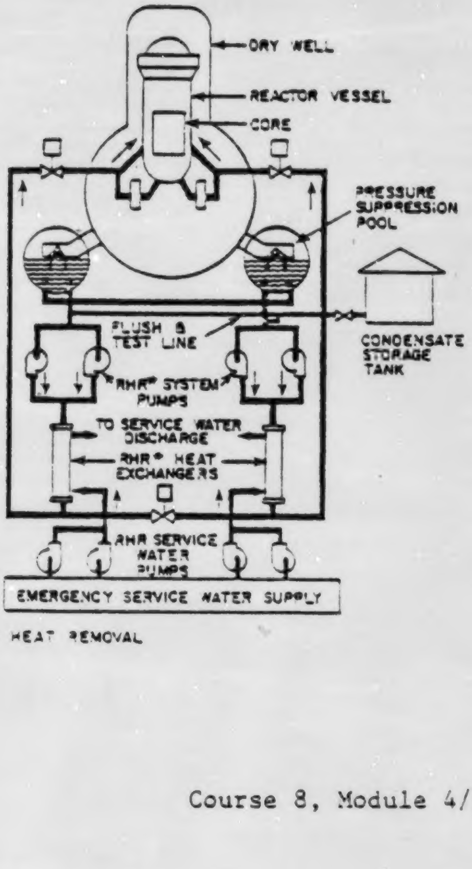

REACTOR-PRESSURE AND LOW-WATER LEVEL SIGNAL
REACTOR-PRESSURE AND LOW-WATER LEVEL SIGNAL
CORE SPRAY HEADERS
REACTOR VESSEL
CORE
DRY WELL
PRESSURE SUPPRESSION POOL
TO RCIC SYSTEM*
TO RHR SYSTEM*
*TO REACTOR HEAT REMOVAL AND COOLANT INJECTION SYSTEMS
CORE SPRAY PUMP
CORE SPRAY PUMP

Figure 8-4-5. BWR core spray system.


DRY WELL
REACTOR VESSEL
CORE
PRESSURE SUPPRESSION POOL
FLUSH & TEST LINE
CONDENSATE STORAGE TANK
"RHR" SYSTEM PUMPS
TO SERVICE WATER DISCHARGE
RHR* HEAT EXCHANGERS
RHR SERVICE WATER PUMPS
EMERGENCY SERVICE WATER SUPPLY

*RHR - REACTOR HEAT REMOVAL

Figure 8-4-6. Coolant injection system.

to prevent a meltdown.

The low-pressure injection system supplements the spray system. It pumps water from the pressure suppression pool directly into the reactor water recirculation loops. This system also is used during normal operation to remove decay heat after shutdown.

In both PWR's and BWR's, water leaking from the primary system is collected and recirculated by the ECCS. In a PWR, the water is collected in the reactor sump and recirculated from there. In a BWR, water collected in the pressure suppression pool includes both primary coolant and water added (by high-pressure ECCS) from condensate water storage tank.

In general, a LOCA or depressurization accident in an HTGCR is not nearly as potentially serious as in a light-water cooled reactor. The large mass of graphite in the core provides a high heat capacity and ensures that core temperature transients are slow and, therefore, controllable.

Emergency core cooling systems for light-water cooled reactors must provide protection in accordance with three specific requirements set forth in Title 10, Code of Federal Regulations, Part 50, Paragraph 46(b):

Peak cladding temperature (calculated for the hottest fuel element) must not exceed 2200°F, which is several hundred degrees below the melting point of fuel or cladding.

Total oxidation of cladding must not exceed 1/6 of total cladding thickness (before oxidation), which ensures at least 5/6 of full strength (well within design safety factor).

Calculated amount of hydrogen from chemical reaction of cladding with water or steam must not exceed 1%

of theoretical maximum (if all cladding around fuel were to react), which ensures that hydrogen concentrations in containment remain below lower explosive limit).

ECCS must be able to continue to keep the core at acceptable temperature levels for long periods; thus, it must be capable of continuous operation for extended periods (until decay heat is no longer capable of producing a meltdown).

RADIATION MONITORING SYSTEMS

Every reactor has emergency systems based on radiation levels or radioactivity concentrations. External levels refer to radiations such as gamma rays or neutrons, which can penetrate a detector (or a person). This radiation commonly is measured in terms of dose rate, flux or exposure rate. Radioactivity concentration is the amount per unit volume (e.g., µCi/ml) in a fluid, such as coolant or containment air.

Specific radiation monitoring systems are called out by 10CFR50 General Design Criteria 60 and 64. These systems control releases of radioactivity to the environment and, as such, may function as emergency systems to limit such releases.

As noted earlier, radiation monitoring systems may be used to actuate shutdown systems. Some may be classed as protection or engineered safeguards, others as systems to prevent personnel exposure or release of radioactivity to the environment.

NUCLEAR INSTRUMENTATION SYSTEMS

Nuclear instrumentation systems are used for 1) reactor protection, 2) monitoring of neutron flux, 3) gamma radiation level detection, and 4) for initiating shutdown actions when indicated. They also indicate reactor status. And some are used for control functions.

All shutdown systems based on neutron monitoring (e.g., flux levels in source, intermediate and power range), as well as in-core gamma radiation detectors, are part of this system and may be used as sensors for shutdown initiation.

Emergency radiation monitoring systems (ERMS) are those that measure area radiation levels or radioactivity in various process fluids (such as secondary system liquids or gaseous- or liquid-waste tanks) and initiate action (or alarm) other than shutdown. In a PWR, a most important emergency radiation monitoring system is the one that measures radioactivity levels in secondary water. This system provides an indication of the condition of steam generator tubes and of demineralizers used in the secondary water system. Ordinarily, these systems provide an alarm, but they may also be programmed to provide a shutdown capability if levels exceed their limits.

Process radiation and area radiation monitoring systems are common to all reactors. Area radiation monitoring systems (ARMS), used to monitor external gamma and neutron radiation levels in specific areas of the plant, protect operating personnel. These systems, usually located in the containment, in rooms or areas where primary coolant piping passes, in areas where waste tanks and filter banks are located and in the control room, are fixed in place, with local readouts as well as central readouts, in either the control room or health physics office.

Major functions of an area radiation monitoring system include:

Continuous monitoring of external radiation levels in a given area.

Signaling abnormal conditions by activation of an alarm.

Providing guidance for personnel required to enter such areas, either as a normal working function or following an accident or other abnormal situation.

A process radiation monitoring system (PRMS) is more properly a radioactivity monitoring system. It measures radioactivity concentration in a particular liquid or gas associated with operation of the plant. Some PRMS, such as primary coolant radioactivity monitors, may function as shutdown systems. Coolant monitors are used also to determine the status of various process auxiliaries, such as demineralizers, filters and other fluid treatments.

In general, PRMS are not emergency systems as such, but are more operational status checks; however, those used in conjunction with effluent discharges are equipped with alarms (or controllers to shut down the process to prevent exceeding technical specification limits and to control environmental discharges). Gaseous streams are far more easily monitored on a continuous basis than liquids.

In summary, a PRMS may perform one or more of the following functions:

- Monitor gaseous radioactivity (directly in GCR and BWR primary systems, and in PWR gaseous-waste storage tanks).
- Measure leakage between systems (steam generators in PWR's, and heat exchangers in BWR's and GCR's).
- Indicate purification system performance (filters on gaseous discharge systems, and demineralizers, in PWR's and BWR's).
- Monitor radioactivity in effluent releases (discharges from low-level liquid radwaste system and gaseous discharges).

EMERGENCY POWER SYSTEMS

An emergency power system is designed to provide sufficient power to ensure safe shutdown if normal on-site power is lost. Plant safety instrumentation loads approach or exceed 100 kW. General Design Criterion 17 (10CFR50, Appendix A) specifies both an on-site and off-site power system to, "... permit functioning of structures, systems and components important to safety." This includes maintenance of core cooling functions, containment and fire protection systems, as well as providing power to shutdown systems.

Electric power is required from two physically separate circuits off-site (in addition to redundant capability on-site) - an off-site system must be available within seconds after an LOCA.

Important aspects of an emergency power system (Figure 8-4-7) are testability and provision for periodic inspection. Important structural and operating components must be accessible to inspection by operating personnel and must be routinely inspected to verify that wiring, insulation, separation and other safety features are in satisfactory condition. Inspection also implies minor testing, such as continuity and physical strength of components and connections.

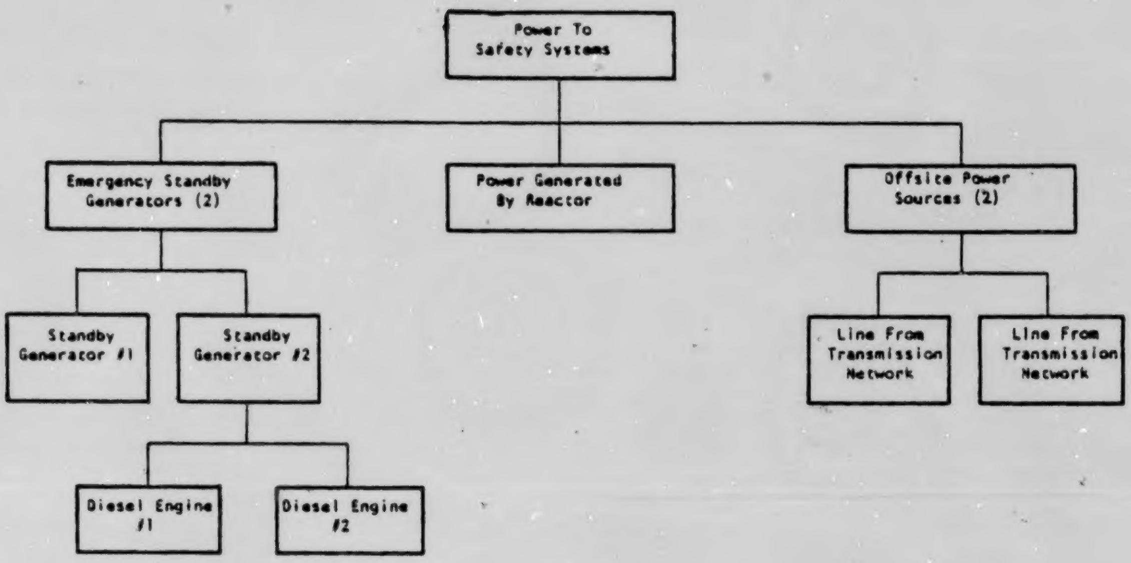

Power To Safety Systems
Emergency Standby Generators (2)
Power Generated By Reactor
Offsite Power Sources (2)
Standby Generator #1
Standby Generator #2
Line From Transmission Network
Line From Transmission Network
Diesel Engine #1
Diesel Engine #2

Figure 8-4-7. Emergency reactor power systems.

The system, as a whole, must be periodically tested to comply with 10CFR50, General Design Criterion 18. This criterion requires testing to verify that systems and their individual components and subsystems are operating in accordance with design and technical specifications. The system must be shown to be capable of operating the appropriate safety systems.

FIRE PROTECTION SYSTEMS

Although the general safety philosophy, as well as 10CFR50, General Design Criterion 3, requires the use of fire-resistant materials and optimum design, fire detection, prevention and suppression systems are necessary adjuncts to reactor emergency systems.

A fire detection system is one that determines the presence of combustion products (e.g., smoke, chemicals or heat).

Fire prevention is the method and physical means whereby combustion itself or the opportunity for combustion is eliminated.

Fire suppression systems act to extinguish fire, whether by cooling, suffocation (removal of oxygen), physical removal of combustibles or a combination of any or all of these three.

In general, a fire protection system includes all three elements: prevention, detection and suppression. But, in common usage, the latter two elements are often considered to constitute this system, since prevention is usually accomplished through design and appropriate actions by operating personnel.

Fire protection systems are provided for all areas containing safety-related equipment, including the control room. Consideration must be given to all aspects of the fire: heat, smoke (including generation of toxic gases and other aerosols) and flame control. In addition to internal automatic systems of the deluge (flood) or sprinkler types, foam systems may be used.

Foam systems require relatively little water and blanket the area with a detergent-based foam that both cools and smothers the fire. Foam also tends to entrap smoke and other particulate matter. And, subsequently, it breaks down to leave little residue. Because it is comparatively dry, with respect to water, it results in relatively little secondary damage to material and components and is thus most useful for electrical system fires. Chemical (dry) and CO_2 systems are also used.

Supplemental to automatic fire protection systems are standpipes, hydrants or pumps that can be connected to hoses for emergency fire fighting operations, pending arrival of off-site apparatus. In some cases, a plant may be equipped with on-site fire fighting capability.

OTHER EMERGENCY SYSTEMS

Many other systems can be classified as reactor emergency systems, depending upon interpretation and breadth imparted to the definition. For example:

Containment heat removal system.
Containment atmosphere cleanup system.
Containment spray system.

CONTAINMENT HEAT REMOVAL

The containment heat removal system, specified by 10CFR50 General Design Criterion 38, may be a heat exchanger through which containment gas is cooled following an LOCA (or other serious accident). This system functions to rapidly reduce temperature and pressure inside the containment, thereby avoiding containment overpressurization and reducing the possibility of breaching containment integrity.

CONTAINMENT ATMOSPHERE CLEANUP

The containment atmosphere cleanup system controls fission products, combustible gases such as hydrogen and oxygen, and other substances that may be accidentally released into the containment. General Design Criterion 41 of 10CFR50 specifies such a system, which may be required to function on an emergency basis.

CONTAINMENT SPRAY

Most power reactors that are light-water cooled are equipped with containment spray systems. This emergency system, if properly designed, can provide the functions of the previously mentioned two systems in addition to providing fire protection. Thus, a single emergency system can provide several functions.

In a typical PWR, an arrangement of spray nozzles is provided near the upper part of the containment, and these are connected to the refueling water storage tank and containment sump. Water from these sources is pumped through the nozzles, providing a spray, which serves to condense steam and thereby reduce temperature and pressure in containment. Also, it washes particulate fission products and radioiodines out of the containment atmosphere (if there has been a release of radioactivity from the fuel). Provision may also be included for addition of chemicals to the spray, such as NaOH to enhance removal of radioiodines.

In a BWR, the spray system is similar, and may also serve as an ECCS.

EXERCISES

1. Outline the sequence of emergency events that would occur following a design basis LOCA in a PWR.
2. A BWR incurs a minor leak in reactor primary piping and undergoes a scram; reactor water level drops gradually but steadily to 80% of original level. What actions, if any, would you expect to occur from actuation of emergency systems?
3. A technician plans to do welding on a broken metal chair in the control room, estimating that the entire operation will take no more than 10 minutes, and probably only 3 minutes. Would you expect problems with any emergency systems? Why?
4. Given a piping schematic of a typical emergency core cooling system (PWR and BWR), trace flow paths and explain operation of each.
5. Given an electrical schematic of a radiation monitoring system and nuclear instrumentation, trace signal path(s) and explain operation of each system.

MATERIALS

None.

PROCEDURES

None.

DATA TABLE

None.

REFERENCE MATERIALS

Harrer, Joseph M. and Beckerley, James G. Nuclear Power Reactor Systems Handbook, Vol. 1, USAEC Publication TID-25952-P1 (1973) and Vol. 2, USAEC Publication TID-25952-P2 (1974).

USAEC documents available by writing Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

Jacobs, I.M. "Safety System Design Technology." Nuclear Safety. 6(1965):231-245.

LaMarsh, John R. Introduction to Nuclear Engineering. Reading, MA: Addison-Wesley Publishing Co., 1975.

Loftness, Robert L. Nuclear Power Plants Design, Operating Experience and Economics. Princeton, NJ: Van Nostrand, 1964.

Masche, G.C. Systems Summary of A Westinghouse Pressurized Water Nuclear Power Plant. Pittsburgh, PA: Westinghouse Electric Co., 1971.

Murray, Raymond I. Nuclear Energy. New York: Pergamon Press, 1975.

Thompson, T.G. and Beckerley, James G. The Technology of Nuclear Reactor Safety, Vols. 1 and 2. Cambridge: The MIT Press, 1964 and 1973.

U.S. Atomic Energy Commission. "Status and Future Technical and Economic Potential of Light Water Reactors," Report WASH - 1082, 1968.

U.S. Nuclear Regulatory Commission. Title 10 - Atomic Energy, Code of Federal Regulations, Part 50.

Government documents available by writing the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

TEST

1. Draw a block diagram of various reactor emergency systems for a PWR; label each system:

2. List emergency reactor shutdown systems; briefly describe functions and general logic of each:

3. List ten parameters used to actuate an emergency shutdown; explain importance of each:
   (1)

   (2)

   (3)

   (4)

   (5)

(6)

(7)

(8)

(9)

(10)

4. Briefly explain basic differences between an emergency core cooling system for a PWR and one for a BWR:

5. Briefly describe, in terms used in this module, an emergency cooling system for a gas-cooled reactor; state principal ways in which it differs from an emergency core cooling system in a water-cooled reactor:

6. Draw a block diagram of an emergency reactor power system; label each block:

7. Define:

Cold water accident.

ECCS.

CACS.

General design criteria.

ARMS.

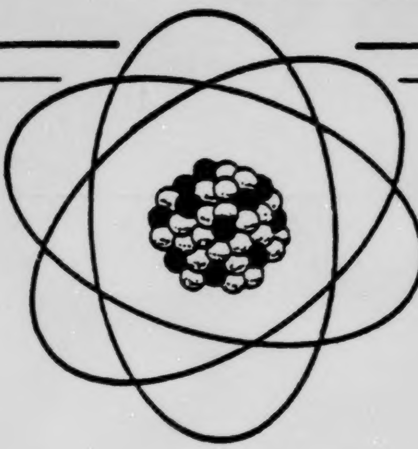
141

PRMS.

Fire detection.

Fire prevention.

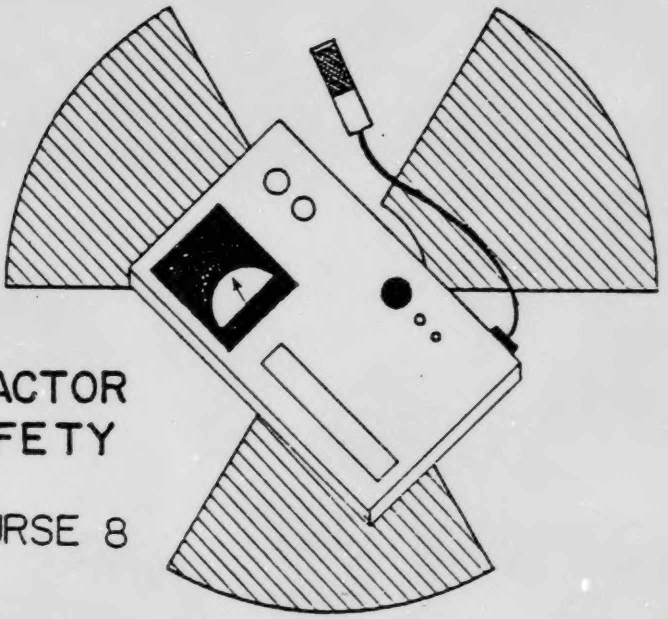
Fire suppression.



NUCLEAR TECHNOLOGY

MODULE 8-5 SAFEGUARDS AND SECURITY. -

RONALD L. KATHREN
PORTLAND GENERAL ELECTRIC COMPANY



REACTOR
SAFETY

COURSE 8

TERC-SW

TECHNICAL EDUCATION RESEARCH CENTER — SOUTHWEST
4201 LAKE SHORE DRIVE WACO, TEXAS

COURSE MODULES

COURSE 8 REACTOR SAFETY

MODULE 8-1	Introduction to Reactor Safety
MODULE 8-2	Reactor Licensing
MODULE 8-3	Reactor Protection Systems
MODULE 8-4	Reactor Emergency Systems
⇨ MODULE 8-5	Safeguards and Security -

Copyright in 1977 by the Technical Education Research Center, Inc. Printed in the United States of America. All rights reserved. These materials, or parts thereof, may not be reproduced in any form without permission.

The materials contained herein were developed pursuant to a contract with the Office of Education, U.S. Department of Health, Education and Welfare: Contract No. 300760356. Contractors undertaking such projects under Government sponsorship are encouraged to express freely their professional judgment in the conduct of the project. Points of view or opinions stated do not, therefore, necessarily represent official Office of Education position or policy.

Technical Education Research Center
Southwest
4201 Lake Shore Drive, Suite 111
Waco, Texas 76710

INTRODUCTION

The nuclear industry evolved primarily from the Manhattan Project, an ultrasecret military project, which developed the atomic bomb.

Secrecy also shrouded the first reactor, which was successfully put into operation December 2, 1942.

Today, this emphasis on secrecy has given way to "security" in its broad sense. Nuclear reactors, whether small research units or large power plant units, take great measures for their physical protection (against sabotage, theft or unauthorized use) to ensure against potential hazards and possible catastrophes. All have security plans of which secrecy now is but a minor ingredient. Similarly, security is applied to all phases of the nuclear fuel cycle.

This module provides an overview of these safeguards and security measures.

MODULE PREREQUISITES

The student should have completed Module 8-4, "Reactor Emergency Systems," and its prerequisites.

OBJECTIVES

Upon completion of this module, the student should be able to:

1. Discuss state and Federal requirements used to limit access to nuclear and radioactive materials.
2. Describe two possible ways thieves may use to obtain nuclear and radioactive materials.
3. Describe how security is incorporated into the selection and training of nuclear plant personnel.
4. Discuss ten procedural and physical safeguards used to prevent theft and sabotage at a nuclear power plant.
5. Describe special security problems associated with various phases of a nuclear fuel cycle other than reactors as described in this module.
6. Define:
    - Nuclear proliferation.
    - SNM.
    - Safeguards.
    - Physical protection.
    - Owner-controlled area.
    - Protected area.
    - Vital area.
    - Co-location.

THE QUESTION OF SECURITY

Nuclear reactors have always been surrounded by an aura of mystery, partly because of security measures and partly because nuclear physics is an unknown to most people. Security originally was dictated by wartime military needs. But peacetime commercial applications have three principal concerns:

Economics.
Control of unique hazards.
Minimization of possible nuclear proliferation.

The first, economics, is considered to a greater or lesser extent by all businesses and individuals; it is the primary reason for locks on doors! A nuclear reactor is an expensive investment; building a large power reactor may cost more than a billion dollars. In return, a large plant, say 1200 MWe, can produce 2.88×10^7 kWh per day, generating a daily revenue of a million dollars or more.

Any commercial endeavor of this size, of necessity, is equipped with certain security features to protect its investment.

Evenso, the other two concerns are more important than the economic considerations. Control of unique hazards infers, of course, radioactivity. Provision must be made to protect the reactor against use by unauthorized persons. For, in spite of automatic safety features, the use by such persons would increase the likelihood of an accident producing damage to the reactor and radiation exposure to reactor personnel. Also increased are the chances of radioactive contamination of the facility and the environment. The probability of such events is initially low, and the potential harm to the public environment even lower. But appropriate security measures can, with little cost or effort, reduce these already low risks to near zero.

Theft of highly radioactive spent fuel elements or reprocessed fuel (particularly plutonium) could be the aim of certain individuals or groups. Appropriate security measures can render such an act virtually impossible.

NUCLEAR PROLIFERATION

The third factor is clearly of the most concern. Nuclear proliferation is a term that has come to mean the increase of nations with nuclear weapons. Reactor fuels, if sufficiently enriched in ^{235}U, ^{239}Pu or ^{233}U, can be used to fabricate nuclear devices.

Other than some research, testing or other special-purpose reactors, reactors do not use fuels with sufficiently high enrichments to be useful in the construction of weapons; however, all uranium-fueled reactors produce plutonium, which can be chemically separated from uranium and used to construct nuclear explosives. The quantities of plutonium produced are surprisingly large. A large power reactor fueled with slightly enriched uranium may produce half a ton of ^{239}Pu in a year. Only a few pounds of ^{239}Pu are necessary to make a nuclear device.

The security concern is with the entire fuel cycle. Small quantities of ^{239}Pu removed at frequent intervals from a fuel fabrication facility soon would constitute a quantity sufficient for a nuclear weapon.

The legal basis for control of special nuclear material (SNM) is that portion of the Atomic Energy Act of 1954 (as amended) and Title 10, Code of Federal Regulations. Special nuclear material is defined as, "...plutonium, uranium enriched in the isotope 233 or in the isotope 235..." Prior to the enactment of the 1954 law, the chance of fabricating nuclear weapons with illicit materials was remote because all special nuclear materials were owned and controlled by the Atomic Energy Commission (AEC). The 1954 law provided for private ownership of SNM, under license. An entire chapter in Title 10 (Chapter 70), devoted to licensing and handling includes references to physical protection during shipment. Detailed requirements for physical protection of plants and materials are given in Chapter 73, "Physical Protection of Special Nuclear Material," and in various other Regulatory Guides.

In addition to the laws and regulations at the federal level, several states have enacted legislation and/or regulations relating to the physical security of SNM and nuclear reactors. In general, these are patterned after the federal requirements, but may be more detailed and comprehensive. Although some legal scholars have questioned the validity of the states' actions, on the basis of federal pre-emption, as of 1977 there has been no legal test in the courts.

INDUSTRIAL SABOTAGE

Until 1967, security requirements were limited to protecting SNM, reactors and fuel-handling facilities from "... sabotage acts by enemies of the United States." In 1967, this basic philosophy was changed by an AEC order relating to an application by the Florida Power and Light Company for a construction permit for a 728 MWe pressurized water reactor at their Turkey Point site, 25 miles south of Miami.

By that order, the utility was required to provide physical security for the plant, including "industrial" sabotage protection in addition to sabotage protection from enemy agents. A few months later, Southern Nuclear Engineering was awarded a contract to study the effects of sabotage acts on public health and safety, determine the vulnerability of nuclear power plants and develop and recommend such additional security features as the study deemed advisable.

The study, published in mid-1968, concluded 1) that plant protection and safety features would be adequate to control individual acts of sabotage and 2) that, for the plant to pose an off-site hazard, a skillfully developed and executed operational plan would be necessary. Such a plan would require saboteur(s) to have considerable technical knowledge and capabilities, and some detailed knowledge of the specific plant. There have been no verified cases of sabotage of operating reactors, although a few instances of damage or similar problems have occurred during construction of power reactors that have been attributed to, or suspected of being, sabotage.

The term security may be thought of as having several key elements:

Nuclear safety.
Physical protection of SNM.
Physical protection of facilities.
Control of nuclear terrorism.
Nuclear safeguards.

Each of these elements, includes planning, engineering, training and qualification of personnel and other administrative requirements, such as the confidentiality of records and plans. The first and last of these elements are generally outside the scope of this module, and will only be mentioned periodically.

(Nuclear safety as such has been the topic of the first four modules in this Course.)

Nuclear safeguards is a special and specific term, usually applied to supervision or overseeing of operations to ensure that nuclear materials are not diverted from peaceful to undesirable military purposes. It is usually used in an international context, relative to the possibility of material being stolen from one country and transported to another that may use it to manufacture weapons it would not otherwise have.

Physical protection is the application of measures to prevent unauthorized and illicit interference with, or sabotage or damage to, nuclear facilities. It also applies to the use of nuclear materials by unauthorized individuals or groups. Its primary concern is with willful and premeditated acts such as theft, ransom, hijacking, terrorism and sabotage. But it also relates to incidental and irrational acts such as trespassing and vandalism.

In some instances, physical protection may be required to protect against legitimate or quasi-legitimate acts by persons exercising various rights and prerogatives as citizens. For example, the right of an individual to refuse to cross a union picket line may alter the security system, and the physical protection plan must be appropriately designed to achieve its goal without interference with this legal and recognized prerogative.

SECURITY OF REACTOR PLANTS

Nuclear power plants have always been subject to certain requirements, which - over the years - have been made more comprehensive and stronger. Smaller reactors, such as those used for teaching and research, have been relatively free of intense security requirements until recently. The primary purpose of reactor security requirements is protection of the public from the consequences of industrial or enemy sabotage; these consequences are not limited to potential hazards from radioactive materials that might accidentally be released to the environment but, more likely, the economic aspects of such events as well as the socio-political consequences. Indeed, it is relatively difficult to damage a nuclear power plant seriously enough to produce a significant danger to the public's health and safety from radioactivity, although many, many scenarios can be developed with this possible but improbable end result.

OWNER-CONTROLLED AREA

Security programs for nuclear power plants are built around three concentric areas, each with a different level of security (Figure 8-5-1). The largest or outermost area, known as the owner-controlled area, has the least stringent level of security precautions. Access control may be limited, and the area may or may not be fenced. For example, a visitors facility, such as an information booth, view point or recreational area, may be within the confines of this outermost area; however, the owner-controlled area must have surveillance by appropriate personnel to ensure that access and use restrictions are not being violated. Provisions exist to remove persons from the area and prevent further access as dictated by security needs.

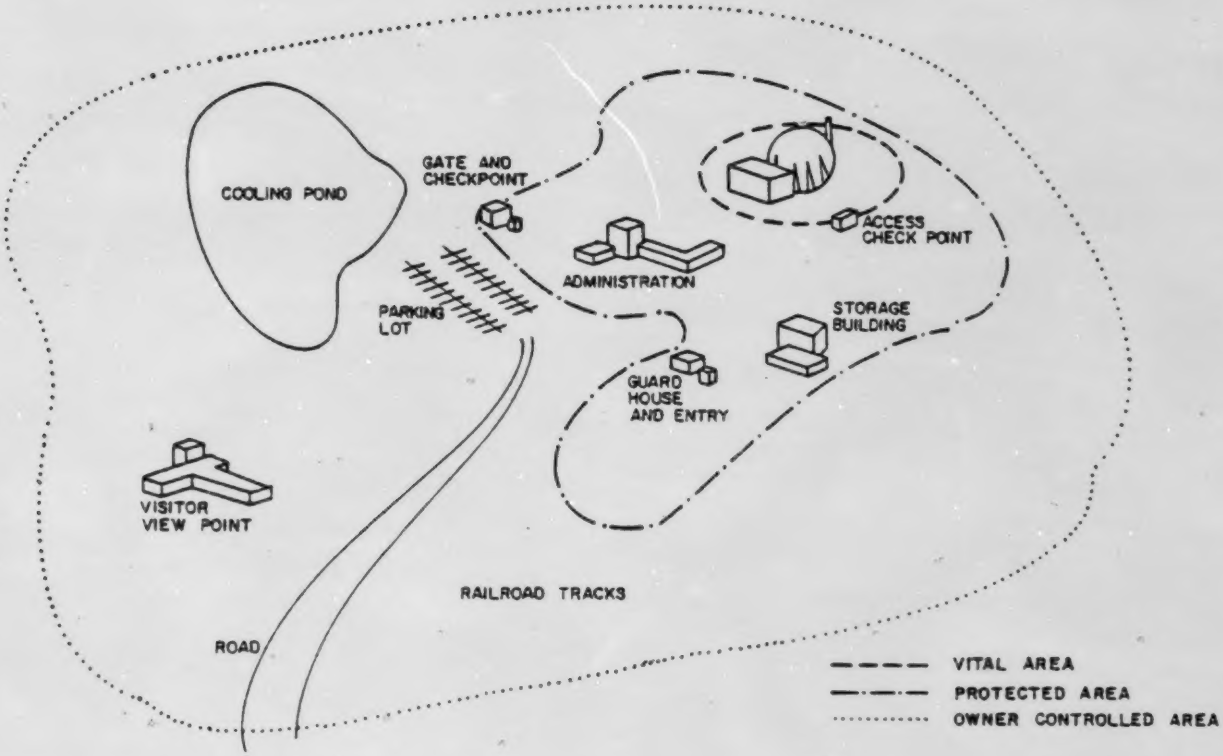

COOLING POND
GATE AND CHECKPOINT
ACCESS CHECK POINT
ADMINISTRATION
PARKING LOT
STORAGE BUILDING
GUARD HOUSE AND ENTRY
VISITOR VIEW POINT
RAILROAD TRACKS
ROAD
VITAL AREA
PROTECTED AREA
OWNER CONTROLLED AREA

Figure 8-5-1. Three safety areas (typical).

PROTECTED AREA

The middle area, known as the protected area, is completely enclosed by fencing or other physical barriers. Because the terrain may not be level, or may include natural water bodies, railroad tracks or other structures, measures must be taken to ensure that barrier integrity is maintained. The physical barrier (i.e., fence or wall) should have a clear area on either side to permit unobstructed view by security personnel.

Security within this restricted area is accomplished by limiting access of both personnel and vehicles. All nonessential vehicles, including those of plant personnel, are located outside the security barrier. Access control is limited to appropriately identified and badged personnel through established control points. Persons authorized for unescorted access are identified by a variety of methods. (The most positive, and least used, method is by means of a device that reads hand or fingerprints or some other unique individual characteristic. The person desiring access may be required to enter a booth or turnstile with room for only one person. Upon entry, the door behind him, leading from the owner-controlled area, locks. To unlock the door to the protected area, the appropriate physical characteristic must be identified. If this characteristic is not identified, the person is trapped and must be released by security personnel.)

Most commonly, individuals are required to pass through check points or gates staffed by security personnel. Personal recognition may be the only criterion for access, or a badge (Figure 8-5-2), bearing the individual's photo may be used. This badge is left at the gate upon exit from the protected area, to be picked up when entry is again required. (The badge never leaves the protected area and is, therefore, "positively" controlled).

In some instances, repair, maintenance and other service personnel, as well as regulatory inspectors and others have need to enter the protected area. Such persons are usually authorized access under escort, with the escort being chosen from among the regular operating personnel. An escorted visitor is required to sign in, after proper identification

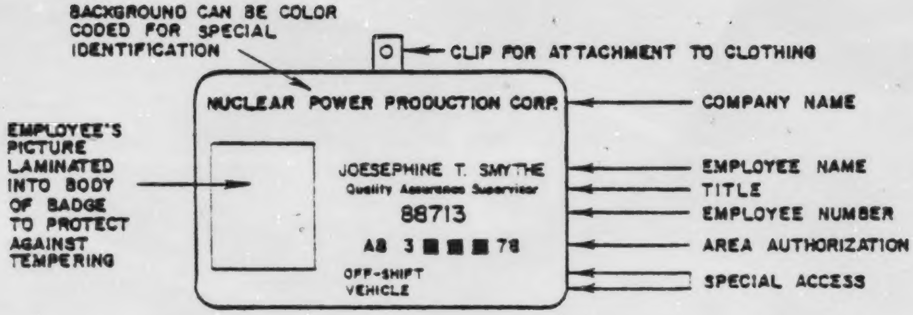

BACKGROUND CAN BE COLOR CODED FOR SPECIAL IDENTIFICATION
CLIP FOR ATTACHMENT TO CLOTHING
NUCLEAR POWER PRODUCTION CORP.
COMPANY NAME
EMPLOYEE'S PICTURE LAMINATED INTO BODY OF BADGE TO PROTECT AGAINST TEMPERING
JOESEPHINE T. SMYTHE
Quality Assurance Supervisor
88713
AB 3 ■ ■ ■ 78
OFF-SHIFT
VEHICLE
EMPLOYEE NAME
TITLE
EMPLOYEE NUMBER
AREA AUTHORIZATION
SPECIAL ACCESS

Figure 8-5-2. Employee's security badge.

(name, purpose of visit, citizenship and other specific information, including the time of entry and exit). A casual visitor may be issued a temporary badge, without photo, noting a necessity for accompaniment by an authorized escort.

In addition, visitors are required to pass through metal detectors; and any briefcases, packages or vehicles are searched prior to entry or departure. Of course, guns, knives, explosives or other weapons are not permitted in protected areas except in unusual or special circumstances. Cameras and binoculars may also be forbidden, since these may be used to gain information about security that would otherwise be unavailable.

Surveillance of protected areas is a continuous and demanding procedure. The perimeter fence might be routinely patrolled on foot by security personnel; television or other electronic surveillance measures might be used to examine physical barriers around the area as well as various locations within it; trained dogs are commonly employed for both patrol and guard functions; electronic "bugs" of various types -

motion, sound and heat sensors and continuity devices - are used as well.

Nighttime lighting must, of course, be adequate to permit visual observation and must also be adequate for closed circuit television or other electronic devices requiring illumination. Frequent use is made of "invisible" (infrared) light or systems employing low-light-level television cameras and amplifiers.

Random patrols are particularly important as a supplement or even in place of routine, regular patrolling, which is more easily circumvented by potential intruders.

In addition to barriers and surveillance aids, the security force must be appropriately trained and equipped to repel and neutralize potential intruders until outside assistance is obtained from recognized law enforcement agencies. The guard force is therefore armed and appropriately trained, and is expected to protect the facility against acts by single individuals and small groups with some knowledge of the facility plans, as well as a larger group without discipline, intent on civil disturbance.

VITAL AREA

Within the just described protected area lies the vital area - those portions of the plant containing equipment and facilities for protection against accidents (that might threaten health or safety) as well as those containing fuel and radioactive materials. Thus, the reactor protection system, containment building and spent-fuel storage pool are natural parts of this vital area.

Access to vital areas and equipment is normally restricted to personnel whose job functions require them to enter and work in such areas. In no case are vital areas opened to casual visitation by unauthorized personnel. Vital areas are equipped with physical barriers to prohibit unauthorized penetration, as well as structural protection from attempts at damage such as small arms fire, fire, small amounts of explosives, ramming by vehicles and similar forces. While the containment may serve this purpose in addition to its primary purposes, special doors, walls, roofs and protective shields may be required for certain vital components. Barriers to deny unauthorized access are also used.

The vital area has additional (and more stringent) surveillance requirements. Personnel badges are examined on entry and exit. Primary monitoring of vital areas and equipment, normally accomplished by operating personnel as part of their duties, is supplemented by electronic monitoring of all access points, including emergency exits and normally unoccupied areas. Response to unauthorized intrusions into vital areas is prompt, designed to protect vital functions as well as to quickly neutralize any potential threat.

In addition to physical protection, such as that provided by security forces, facility design and alarm devices, the total security program contains other elements. These include various administrative aspects, such as planning, personnel selection and training, procedures and facility drills and audits.

Security is an important independent function and should be the explicit responsibility of an appropriately qualified individual. The security manager or director is responsible for establishment of the technical and maintenance requirements for the program. This responsibility includes personnel (selection and training), physical facilities and development of a total security plan (of which procedures and agreements are a part).

Daily operational responsibility for security, however, is properly that of the plant superintendent. Under this individual's guidance security needs can be coordinated with those of other operating functions.

SELECTION AND TRAINING OF EMPLOYEES

An important aspect of plant security is selection and training of employees. Because of the potential for error or misjudgment, each employee is carefully screened for suitability. This screening includes an investigation (security check) of the individual's background to verify statements made on the employment application. It also attempts to determine if the person has character traits that might affect ability to properly perform assigned duties (for example, alcoholism or periodic bouts of drunkenness, excessive debt, dependence on drugs, or hidden events (instabilities) that could subject the individual to blackmail).

Similarly, the individual's medical condition and history - both physical and mental - are evaluated. A person displaying obvious signs of mental instability would be disqualified if there were reasonable cause to assume this problem might affect ability to discharge duties of the position in an appropriate manner. The types of background investigation may vary somewhat with work assignments, but generally apply to all plant personnel. Even those employees without access to vital or other sensitive areas may have available to them important details regarding plant operations, which could be of use to outsiders bent on (industrial) sabotage.

All personnel should be given training regarding plant security procedures and conduct of operations. Such training ordinarily includes specific items of personal interest, such as how to display the security badge and parking and access restrictions. Also, general purposes and principles of security, as well as the role of each individual employee and the special role of the security force are included.

Security personnel are provided with much more intensive training, including operation and testing of various security systems, devices and alarms in use, legal and regulatory requirements, civil rights, weapons usage and qualification, and self-defense. In addition, the security force receives certain basic law enforcement training, including traffic and crowd control, emergency first aid, fire fighting, disaster control, civil defense, communications and criminal law; knowledge of these subjects would be of particular value in the event of an emergency. Security forces, generally, are made knowledgeable about basic radiation protection, and are acquainted with the health physics staff and its requirements, as well as with the facility emergency plan.

Selection of security personnel requires special consideration, with emphasis on physical condition (those who cannot meet certain physical exertion requirements may be disqualified). Security personnel generally are required to meet certain minimum standards relating to vision and hearing. Their psychological and motivational characteristics may be closely scrutinized, also.

SECURITY PLAN

At the heart of the overall reactor security program is the security plan. This documented comprehensive plan includes a description of the design and operation of all security devices and alarms, response actions to various threats, and security procedures. Because of the sensitive nature of this document, its distribution is rigidly controlled and limited; even security personnel may have access to only portions of the plan.

Security procedures, which are a part of the plan, are the basic operating guide for the security forces. ANSI Standard N18.17 lists 19 specific subject areas for security procedures (included in those listed in Table 8-5-1).

TABLE 8-5-1

SPECIFIC SUBJECT AREAS FOR SECURITY PROCEDURES

(adapted from the second reference,
with additions)

1. General and specific post orders
2. Contraband
3. Bomb or other overt threats
4. Civil disturbances
5. Security communications
6. Employee security training
7. Security force duties and responsibilities
8. Incoming package and material control
9. Intrusion alarm response
10. Lock and key procedures
11. Patrol procedures
12. Personnel identification
13. Access control (security)
14. Special procedures or instruction for local law enforcement agencies
15. Vehicle traffic and parking control
16. Surveillance requirements and procedures
17. Testing and maintenance of security systems
18. Reporting requirements
19. Audit procedures
20. Security during operational emergencies
21. Support from off-site security forces
22. Aircraft and other hazards
23. Safety

Note: This list is by no means exhaustive.

Another important aspect of total security relates to nuclear plant design. Simply stated, a plant should be initially designed with security in mind, and a detailed discussion of preliminary planning and design for security is included in the Preliminary Safety Analysis Report (PSAR). The PSAR data includes plans for incorporation of physical protection, details and drawings of physical barriers, alarms and other means of controlling protected and vital areas, and a preliminary indication of responsibilities. The Final Safety Report (FSR) includes the security plan described above.

Although security information is part of the licensing process, it is submitted separately and withheld from public disclosure in accordance with established regulations (Title 10, Part 2 of the Code of Federal Regulations).

SECURITY DURING OTHER PHASES OF THE FUEL CYCLE

Security requirements are associated with other phases of the nuclear fuel cycle (Figure 8-5-7). In general, security measures are similar to those used for nuclear power plants. In some instances, more extensive efforts may be required to protect fuel from diversion. As mentioned before, the term safeguards is usually applied to protection of fuel from diversion.

MINING AND MILLING STAGE

Uranium mining and milling require no particularly extensive security effort. Uranium ore, even after concen-

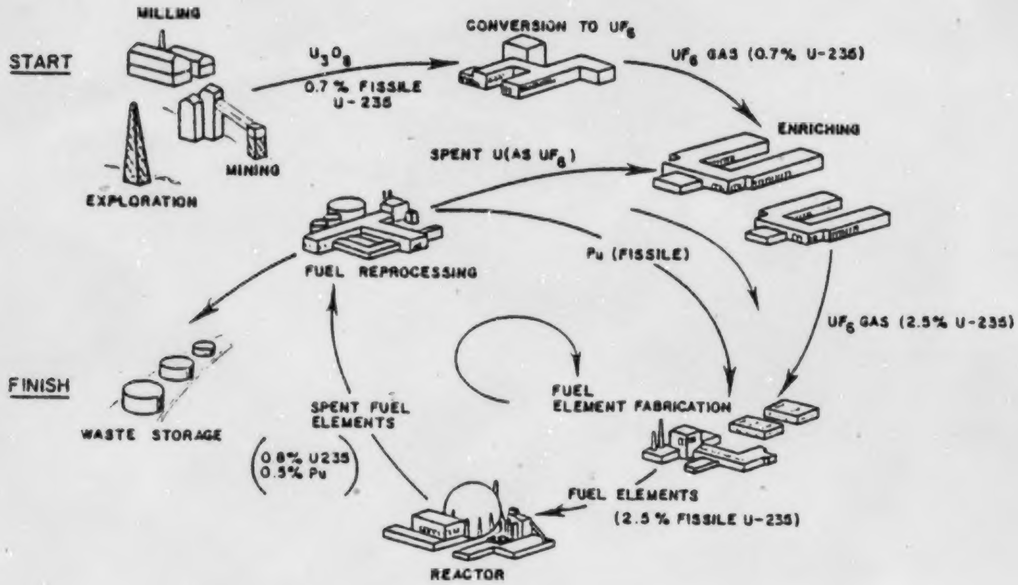

MILLING
START
U_3O_8
0.7 % FISSILE U-235
CONVERSION TO UF_6
UF_6 GAS (0.7% U-235)
ENRICHING
MINING
EXPLORATION
SPENT U(AS UF_6)
FUEL REPROCESSING
Pu (FISSILE)
UF_6 GAS (2.5% U-235)
FINISH
WASTE STORAGE
SPENT FUEL ELEMENTS
(0.8% U235 0.3% Pu)
FUEL ELEMENT FABRICATION
FUEL ELEMENTS (2.5 % FISSILE U-235)
REACTOR

Figure 8-5-7. Nuclear fuel cycle.

tration, is too dilute to be of value for the production of nuclear explosives, and enrichment is an expensive and highly complex technical process. Hence, general and relatively simple industrial security measures are all that are necessary. Consideration should be given to protection of the facilities and extracted ore from harassment and damage designed to disrupt the nuclear fuel cycle.

Although uranium ore is valuable, the market is quite limited and generally restricted to fairly large quantities. Likewise, the radiological hazard potential of the ore is negligible. The theft problem is by comparison considered minimal.

Unless the enrichment facility has a capability for making highly enriched uranium, it has few special security requirements. Most power reactors are fueled with uranium that is enriched by only 2 to 3%. Enrichment to 70% or more is required for weapons-grade material. Thus, at this stage of the cycle, protection against industrial sabotage is probably the single most important security criterion.

FUEL FABRICATION STAGE

At the fuel fabrication stage, special security measures may become necessary. This stage in the cycle is more crucial to reactor operation, and damage to these facilities could seriously impact reactor fuel availability. Also, if plutonium fuels are being fabricated, a greater likelihood of theft exists; plutonium is relatively easily separated from uranium and, if sufficiently pure, ^{239}Pu may be used for the manufacture of nuclear explosives directly.

In addition to the possibility of diversion for use in weapons, plutonium presents yet another potential problem. It is highly toxic and could be the object of terrorist acts for that end use.

FUEL REPROCESSING STAGE

The fuel reprocessing phase of the cycle also poses certain special security problems. Plutonium is separated from spent fuel at this stage, as are high level radioactive wastes. The wastes may remain in liquid form for several years, and measures must be taken to protect them from theft, from release by terrorist, and from other acts.

Protection of the fuel reprocessing facilities requires extensive security because of the nature of the activity and the potential for hazard to the public if the facilities should be damaged by irresponsible acts.

While no high-level waste disposal method has been selected for use in the United States, it is likely that whatever option is chosen will require some security measures, but nowhere approximating the extent of those required at the fuel fabrication or reprocessing phases. Once high-level wastes have been solidified, their hazard potential is greatly reduced - their significance as a terrorist weapon diminishes respectively. Moreover, solidified wastes, because of their bulk and associated shielding, tend to minimize theft potential. There does exist, however, a finite potential for terrorism and psychological acts, and security programs will have to be designed with these possibilities in mind.

In general, protection of special nuclear material at all phases of the nuclear fuel cycle is accomplished by measures similar to those used for reactors. SNM is confined to specific areas, physically isolated, with access restricted to appropriate persons. Storage vaults are equipped with intrusion alarms, and exit points are staffed by armed guards. Special monitoring devices are used to ensure that personnel are not removing quantities of SNM on their persons or in their belongings. Vehicles leaving the area are searched and monitored, as are all packages and containers.

MATERIALS ACCOUNTING

A measure of the effectiveness of the safeguarding of fuel materials can be determined by material control and accounting. These techniques also provide the mechanisms for determining the type of material lost, the amount, the approximate time and location.

Material balance accountability (MBA) is required under the provision of Title 10, Part 70 of the Code of Federal Regulations; licensees holding more than 380 grams of SNM are required to conduct physical inventories. Material balance is a means of determining how much SNM is unaccounted for; material unaccounted for (MUF) is calculated by subtracting the measured quantity on hand (ending inventory, EI) from the amount at the start of the accounting period (the beginning inventory, BI), then taking into account any amount added, A:

$$\text{Material Unaccounted For} = \text{Beginning Inventory} + (\text{Amount Added}) - (\text{Ending Inventory}).$$

$$MUF = (BI + A) - (EI). \quad \text{Equation 8-5-1}$$

Regulations also require the keeping of detailed records regarding handling and transfer of SNM.

Concern is sometimes voiced with regard to quantities of SNM that apparently are missing and not accounted for. Often these quantities are presumed to have been stolen. More likely, these "losses" are attributable to measurement errors. For example, suppose a fuel fabrication facility handles 6000 kg of Pu per year, performing all sorts of mechanical operations and generating several tons of waste containing an estimated few hundred grams of Pu. Exact measurement of the amount of the Pu in the waste is difficult and, for the sake of safety, this quantity may be slightly overestimated. The 6000 kg is handled in much smaller amounts and, since no scale is perfectly accurate, tiny measurement errors tend to creep in. These errors become magnified after several thousand, individual weighing operations.

Consider, for example, a scale accurate (on the low side) to 1 part in 1000, or 0.1%, used for weighing final fuel elements, each weighing 1 kg. The error per weighing would be 1 g and, after 6000 weighings, 6000 g would be MUF.

An obvious weakness of the weighing system is illustrated by the following example.

EXAMPLE

Given: A slab of Pu weighing 10 kg, to be cut into 20 equal pieces, with each piece to be made into 20 fuel pins; scale is 1 part in 1000.

Find: Total MUF.

Solution:

PIECE NO.	WEIGHT
1	500.72 g
2	498.64
3	498.83
4	501.08
5	497.96
6	498.31
7	499.99
8	496.28
9	500.48
10	498.21
11	496.51
12	498.87
13	499.03
14	500.39
15	502.01
16	497.20
17	497.71
18	499.09
19	496.81
20	494.88
TOTAL	9971.00 g

Original Weight = 10,000 g.

Thus, 29 g may be assumed to have been lost in cutting. But, when the chips are weighed, they weigh only 20 g. Hence, 9 g are MUF. (A similar effect might occur in the next operation.)

SHIPMENT STAGE

Perhaps the most significant security problem relates to the protection of SNM and high-level radioactive wastes during shipment. Five-hundred or more civilian shipments containing strategically important quantities of SNM are made each year in the United States. To date, none has been the target of theft or sabotage attempts.

Special security precautions during shipment are designed to accomplish the following:

Ensure that vehicle location is known at all times.

Provide for delay (or slowing down) of entry into vehicle, thus permitting more time for aid to arrive.

Detect deviations from prescribed routings (without approved action by convoy personnel).

Have in readiness a force sufficient to rescue shipment if a theft or hijack attempt is made.

These goals can be met by a variety of means:

Equipping shipment or container with an automatic transmitter to permit its location to be ascertained.

Providing locking devices for vehicles and containers to prevent easy access.

Equipping vehicles with automatic disabling devices to prevent movement once it has been interrupted.

Shipments involving significant quantities are accompanied by two or more armed guards and use preplanned routings to avoid potential trouble areas. Guards may ride in separate escort vehicles. Both the truck and the escort vehicle must be in communication, and periodic checkin by radio-telephone and at certain checkpoints is required. Vehicles carrying SNM or high-level wastes may be marked on tops and sides to facilitate identification from the air. Locks and seals are provided for containers and vehicles.

Perhaps the most effective means of limiting potential security risks associated with transportation is co-location of nuclear facilities. That is, fuel fabrication and reprocessing facilities may be situated on the same site as the power reactor, or perhaps several power reactors. All could be located inside a single protected area, thus providing certain other security advantages in addition to virtually eliminating the transportation security problem. (Co-locate may be neither economically nor environmentally a wise decision, however, and considerable study of this option is required to fully assess its potential benefit.)

EXERCISES

1. Calculate MUF for a plant that had 83.641 kg of ^{235}U at the start of the year, shipped out 127 kg as fuel pins, added 29.014 during the year, and had an inventory of 13.993 kg on hand at the end of the year.
2. Why are both physical and psychological examinations important to security efforts?
3. Briefly outline the "three concentric area" concept of reactor security.
4. What constitutes SNM?

MATERIALS

None.

PROCEDURES

Divide the class into two groups, A and B.

1. Group A: Devise a security scenario for a shipment of spent fuel, according to information given in this module.
   Group B: Devise a terrorist incident scenario attempt to circumvent security in the shipment of spent fuel.
2. Group A: Devise a theft scenario for 10 kg of Pu from a fuel fabrication plant.
   Group B: Devise a security scenario, according to regulations, that would circumvent a theft attempt from a fuel fabrication plant.

DATA TABLE

None.

REFERENCE MATERIALS

American National Standards Institute. "Administrative Controls for Nuclear Power Plants." ANSI Standard 18.7, 1972.

________. "Industrial Security for Nuclear Power Plants." ANSI Standard 18.17, 1973.

________. "Selection and Training of Personnel for Nuclear Power Plants." ANSI Standard 18.1, 1971.

ANSI Standards available by writing the American Society of Mechanical Engineers, United Engineering Center, 345 East 47th Street, New York, NY 10017.

Atomic Industrial Forum. "Protection of Special Nuclear Materials and Facilities." MF Committee on Nuclear Materials Safeguards. February, 1973.

Hough, C.G., et al. "Physical Protection of Nuclear Material." *Industrial Atomic Energy Association Bulletin* 17 (April, 1975) 2:28.

________. "Physical Protection of Radioactive Material in Transport." *Industrial Atomic Energy Association Bulletin* 17 (April, 1975) 2:44.

Morauriecki, Wojciech. "IAEA's Approaches to Physical Protection of Nuclear Materials." *Industrial Atomic Energy Association Bulletin* 18 (February, 1976) 1:25.

U.S. Atomic Energy Commission. *Code of Federal Regulations*, Title 10 - Atomic Energy, Parts 2, 50, 70 and 73.

See especially 70, "Special Nuclear Material," and 73, "Physical Protection of Special Nuclear Material."

Available by writing the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

U. S. Nuclear Regulatory Commission. "Protection of Nuclear Power Plants Against Industrial Sabotage." Regulatory Guide, No. 1.17, June, 1973.

________. "Requirements for the Physical Protection of Nuclear Power Reactors." Code of Federal Regulations, Title 10 - Atomic Energy, Federal Register 42, No. 37, 24 February 1977.

USNRC publications available by writing the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

Willrich, Mason and Taylor, Theodore B. Nuclear Theft: Risks and Safeguards. Cambridge, MA: Ballinger Publishing Co., 1974.

1. Describe what state and Federal requirements are used to limit access to nuclear and radioactive materials:

2. Discuss two ways thieves might attempt to obtain nuclear and radioactive materials:

3. How is security incorporated into selection and training of nuclear plant personnel?

4. Describe ten procedural and physical safeguards used to prevent theft and sabotage at a nuclear power plant:

5. As discussed in this module, list stages of a nuclear fuel cycle (exclude reactor) and note special security problems associated with each:

6. Define:

Nuclear proliferation.

SNM.

Safeguards.

Physical protection.

Owner-controlled area.

Protected area.

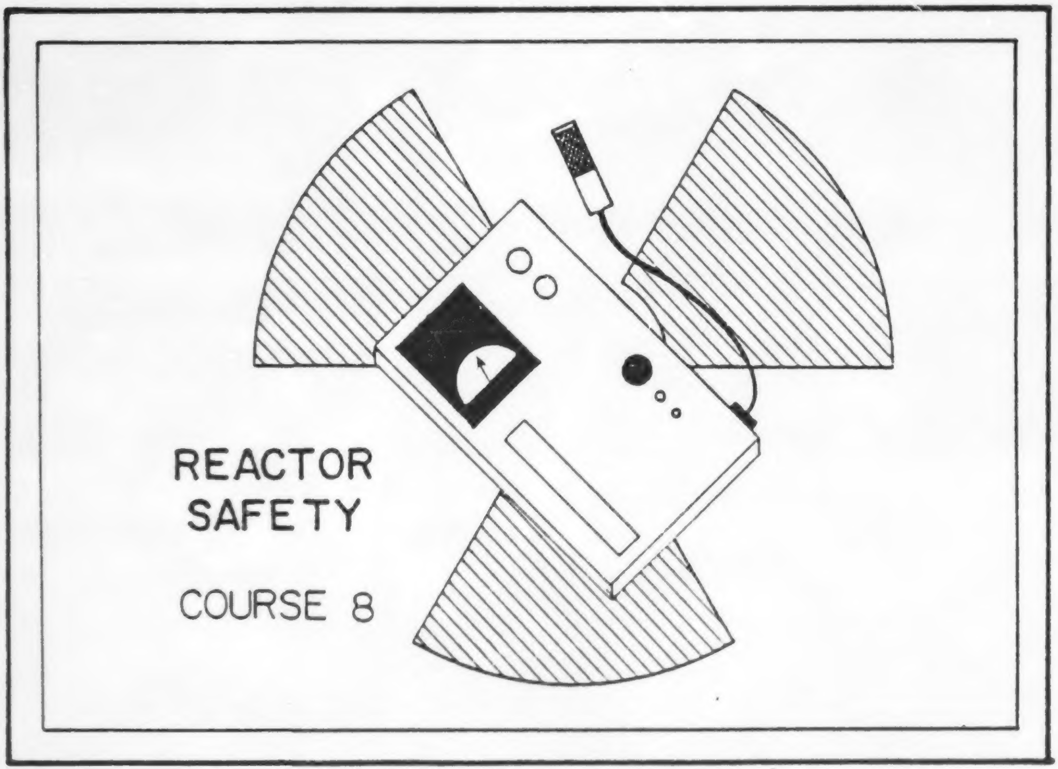
Vital area.

Co-location.

NUCLEAR TECHNOLOGY

INDEX

COURSE 8 - REACTOR SAFETY


REACTOR
SAFETY
COURSE 8

TERC-SW

TECHNICAL EDUCATION RESEARCH CENTER — SOUTHWEST
4201 LAKE SHORE DRIVE WACO, TEXAS

NUCLEAR TECHNOLOGY SERIES
INDEX
for
COURSE 8, REACTOR SAFETY (FIVE MODULES)

NOTE: Each module in this Course is numbered separately, and the page numbers begin with page 1 in each module. Therefore, this Index lists for each entry the module number (underlined), followed by a comma and the page number. Figures and tables are listed by their numbers, followed by the module and page number in parentheses. A Master Index is available in a separate volume. This general index merges all index entries from the 35 Nuclear Courses. It is a valuable research tool, with which the student or researcher can locate all the references to any subject within the 35 Courses.

Access control
  and protected area security, 8-5, 10
  of vital area, 8-5, 12, 13
Accident
  analysis, 8-2, 25
  classification, 8-1, 19; Table 8-1-1 (8-1, 20)
  postulated, 8-1, 18
Advisory Committee on Reactor Safeguards
  review of permit applications by, 8-2, 15
Area radiation monitoring systems
  functions of, 8-4, 18, 19
Atmosphere cleanup system
  containment, 8-4, 24
Atomic Energy Act
  provisions of, 8-2, 5, 6
Atomic Energy Commission
  responsibilities of, 8-2, 5-8
Atomic Safety and Licensing Board
  and construction permits, 8-2, 16, 17
Atomic Safety Licensing and Appeals Board
  appeals through, 8-2, 17

Barriers
  multiple, 8-1, 7

Code of Federal Regulations
  arrangement of, 8-2, 9; Table 8-2-1 (8-2, 10)
Cold water accident
  discussion of, 8-4, 5, 6
Construction permit
  application for, 8-2, 14, 15

Department of Energy
  formation of, 8-2, 9
Design
  basis accident, and safety design criteria, 8-1, 12
  criteria, source of, 8-1, 14
  logic in, 8-3, 16
  inherent safety in, 8-1, 5; use of fail-safe mechanisms for, 8-1, 6

Emergency core cooling system
  in boiling water reactor, 8-4, 13, 14; Figs. 8-4-5, 6 (8-4, 15)
  general description of, 8-4, 11
  in light-water reactor, 8-4, 16, 17
  parameters for, 8-4, 16, 17
  in pressurized water reactor, 8-4, 11-13
Emergency power system
  description of, 8-4, 20, 21
Emergency radiation monitoring system
  description of, 8-4, 17
Emergency system
  discussion of, 8-4, 3, 4
Energy Reorganization Act
  provisions of, 8-2, 8, 9
Environmental monitoring program
  description of, 8-2, 29-32
Environmental report
  preparation of, 8-2, 27; Fig. 8-2-2 (8-2, 28)
Environmental technical specifications
  description of, 8-2, 25
Exclusion area
  definition of, 8-1, 16; Fig. 8-1-4 (8-1, 17)

Fault-tree analysis
  definition of, 8-1, 21, 22
Fees
  license application, for reactor, 8-2, 20
Final environmental statement
  and permit application review, 8-2, 16
Fire
  protection systems, 8-4, 22

Geological site
  and reactor safety, 8-1, 16

Heat removal system
  containment, 8-4, 23-24
Hydrology of site
  and reactor safety, 8-1, 16

Law
  definition of, 8-2, 6

License
  operating, application for, 8-2, 18-20; class 103, 8-2, 19; class 104, 8-2, 19
  operator, application for, 8-2, 32; description of, 8-2, 33; senior, 8-2, 33
Low-population zone
  definition of, 8-2, 16, 17

Material accounting
  as part of fuel cycle security, 8-5, 20, 21
Meteorology of site
  and reactor safety, 8-1, 16
Multiplicity
  of safety systems, 8-1, 8, 10

National Environmental Policy Act
  effect of, on reactor licensing procedure, 8-2, 26, 27
Negative temperature coefficient
  in reactor safety, 8-1, 6
Nuclear instrumentation systems
  functions of, 8-4, 17, 18
Nuclear Regulatory Commission
  responsibilities of, 8-2, 9

Operator
  reactor, senior, 8-2, 33
Owner-controlled area
  of reactor security, 8-5, 8; Fig. 8-5-1 (8-5, 9)

Permit
  construction, application for, 8-2, 14, 15
Physical protection
  and reactor security, 8-5, 7
Population center distance
  definition of, 8-1, 17
Preliminary Safety Analysis Report
  content of, 8-2, 21-26
Process radiation monitoring system
  description of, 8-4, 19
  function of, 8-4, 20
Protected area
  of reactor security, 8-5, 9-12
Protection system
  fire, 8-4, 22
  reliability of, 8-3, 15, 16
  testing and maintenance of, 8-3, 20, 21
  use of fail-safe design in, 8-3, 17
  use of general coincidence logic in, 8-3, 19
  use of logic in, 8-3, 18, 19

Quality assurance
  discussion of, 8-1, 13, 14

Radiation monitoring system
  discussion of, 8-4, 17, 18
Rasmussen Report
  as reactor safety study, 8-1, 19
Reactor protection
  accuracy of instrumentation and, 8-3, 10
  basic criteria for, 8-3, 3
  design of, 8-3, 5-7
  engineered safety features of, 8-3, 3
  environmental factors and, 8-3, 13
  instrumentation range and, 8-3, 11
  plant variables and, 8-3, 8
  reactor shutdown system for, 8-3, 3
  redundant systems for, 8-3, 16
  reliability of, 8-3, 13, 14
  response time and, 8-3, 12
  safety margin in, 8-3, 9; Fig. 8-3-3 (8-3, 10)
  standard setting bodies for, 8-3, 8
  system analysis procedure, 8-3, 4, 5
  system parameters for, 8-3, 9
  system and plant interaction, 8-3, 14, 15
  systems, types of, 8-3, 3
Reactor security. See Security
Regulation
  definition of, 8-2, 7
  of nuclear reactors, 8-2, 11-13
Regulatory Guides
  by Nuclear Regulatory Commission, 8-2, 9, 11

Safeguards
  and reactor security, 8-5, 7
Safety
  evaluation report, 8-2, 15, 16
  implementation of, 8-1, 14
  reactor, in design phase, 8-1, 11-15; design objectives of, 8-1, 11, 12; philosophy of, 8-1, 5; reactor siting and, 8-1, 15, 16
  systems, redundancy in, 8-1, 8-10
  technical specifications, 8-2, 24
Scram
  automatic, 8-4, 5
  definition of, 8-4, 4, 5
  high-temperature gas-cooled reactor, 8-4, 9, 10
  manual, 8-4, 5
  overpower, 8-4, 6; Fig. 8-4-2 (8-4, 7)
  systems, types of, 8-4, 6; Table 8-4-1 (8-4, 8)
Security
  fuel, during fabrication, 8-5, 19; during reprocessing, 8-5, 19, 20; during shipment, 8-5, 23, 24; during mining and milling, 8-5, 17, 18
  protection area, 8-5, 9-12; check point in, 8-5, 10
  reactor, concerns of, 8-5, 3, 4; for control of nuclear materials, 8-5, 4, 5; key elements of, 8-5, 6; plan for, 8-5, 15-17; and protection against sabotage, 8-5, 5, 6; employees for, 8-5, 14, 15
Seismology of site
  and reactor safety, 8-1, 16

Shutdown
  system, 8-4, 4
Siting of reactor
  and reactor safety, 8-1, 15
Spray system
  containment, 8-4, 24, 25
Surveillance
  of protected area, 8-5, 11, 12
  of vital area, 8-5, 13

Vital area
  for reactor security, 8-5, 12, 13;
    Fig. 8-5-1 (8-5, 9)

WASH-1400
  findings in, 8-1, 23-26
  reactor safety study, 8-1, 21
WASH-740
  reactor safety study, 8-1, 19-21